EMERGING TECHNOLOGIES AND THEIR IMPACT
May/June 2006
www.technologyreview.com

Nominated for a National Magazine Award for General Excellence

Technology Review

AN MIT ENTERPRISE

Inside the Spyware Scandal

When Sony BMG hid a "rootkit" on their CDs, they spied on you and let hackers take over your computer. What were they thinking?

BY WADE ROUSH

Page 48

technology
review
Published by MIT

Your potential. Our passion.™

Microsoft

A Global Hotel Company Analyzing 1.4 Million Records a Day. Running On Microsoft SQL Server 2005.

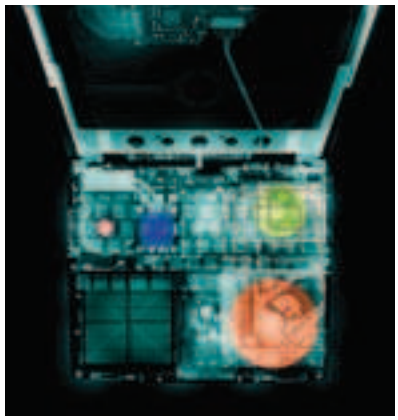
How does Hilton forecast demand for its 370,000 rooms and its catering services? They import data from six systems into one data warehouse requiring 7 million rows, and running on SQL Server™ 2005 with 99.98% uptime.* See how at **microsoft.com/bigdata**

Microsoft® SQL Server™ 2005

*Results not typical, and are based on use with Windows Server™ 2003 Enterprise Edition. Availability is dependent on many factors, including hardware and software technologies, mission-critical operational processes, and professional services.

Contents

Volume 109, Number 2



Cover photo by David Arky

Features

Forward

Hack

Q&A

Notebooks

Photo Essay

Reviews

Demo

From the Labs

36 Years Ago in *TR*

Vinton G. Cerf
Vice President and Chief Internet Evangelist
Google

Amy Wu
Computer Science Student
Stanford University

Benjamin Mako Hill
Research Assistant
MIT Media Laboratory

Maria Klawe
Dean of Engineering
Princeton University

ACM: KNOWLEDGE, COLLABORATION & INNOVATION IN COMPUTING

Uniting the world's computing professionals, researchers and educators to inspire dialogue, share resources and address the computing field's challenges in the 21st Century.

Association for Computing Machinery
Advancing Computing as a Science & Profession
www.acm.org/learnmore

Contributors

Philip E. Ross, who has been a science and technology journalist for 17 years and has contributed to such publications as *Forbes*, *IEEE Spectrum*, and *Scientific American*, was reminded of an old story as he wrote about nanotoxicity for this issue *(see "Tiny Toxins," p. 66)*. "In 1991," he says, "the late Richard Smalley told me about the most important single clue he found on the way to his 1996 Nobel Prize in chemistry. He and his colleagues were studying mass spectrographs of white-hot carbon soot, and they found a sharp spike at a point corresponding to the weight of 60 carbon atoms. To find out why that magic number was so stable, Smalley pieced together paper polygons on his kitchen floor to get the famous soccer ball shape of a buckminsterfullerene. I remember him saying, as an afterthought, that if precisely shaped soot could have extraordinary properties, then it ought to be possible to devise bioactive forms. He was thinking about making drugs, but I credit him with foreseeing today's debate over the threat of nanotoxins. What is a toxin, after all, but a drug gone bad?"

Amanda Schaffer wrote this month's review of recent media attention paid to clinical drug trials *(see "Drug Trials and Error," p. 70)*. "I still can't get over the fact that *Harper's* allowed an AIDS denialist like Celia Farber to write an extended examination of AIDS-related drug trials," she says. "Beyond pointing out the problems with Farber's piece, though, I wanted to get to a more sensible critique of drug trials in the developing world." Schaffer writes about science and medicine for *Slate*. She has also contributed articles and reviews to *Bookforum*, the *Boston Review*, the New York *Times*, and other publications.

David Arky created the image for this month's cover. "Ever since I discovered that my Uncle Morris has patented a device for holding a patient's head still while having a medical x-ray done," he says, "I have been hooked on using the x-ray 'camera' for artistic purposes." Arky creates still-life and x-ray images for *Men's Health*, the New York *Times Magazine*, and *O, The Oprah Magazine*, among others, and he has created advertisements for such brands as Fresca, Hewlett-Packard, Compaq, and Amgen.

2005 SPONSORS

accenture
High performance. Delivered.

Akamai
The Trusted Choice For Online Business℠

BRIDGE BANK

ENDECA

IBM

KPMG

LEWIS global public relations

MAYFIELD

VLAB
MIT•Stanford Venture Lab

MONTGOMERY & CO
INVESTMENT BANKING

Morgan Lewis
COUNSELORS AT LAW

NETSUITE
ONE SYSTEM. NO LIMITS.

palmsource

FENWICK & WEST LLP

Invest Northern Ireland

Silicon Valley Bank & SVB Alliant

PR Newswire
United Business Media

Novell

realmsystems

YAHOO!

AlwaysOn
the insiders' network

STANFORD TECHNOLOGY VENTURES PROGRAM

PRESENT

MEET THE TECH INDUSTRY'S TOP LEADERS AND INNOVATORS...

SAVE THE DATE

AO2006: THE INNOVATION SUMMIT @ STANFORD

JULY 25–27, 2006 | FRANCES C. ARRILLAGA ALUMNI CENTER, STANFORD UNIVERSITY

ALWAYSON'S ANNUAL INNOVATION SUMMIT @ STANFORD IS THE MOST POWERFUL THOUGHT LEADER AND BUSINESS DEVELOPMENT CONFERENCE IN SILICON VALLEY.

EACH YEAR THE SUMMIT FOCUSES ON THE SWEET SPOTS IN THE TECHNOLOGY MARKETS – WHERE INNOVATION IS DISRUPTING BEHAVIOR AND CREATING NEW BUSINESS OPPORTUNITIES.

PREVIOUS STANFORD SUMMIT SPEAKERS

- **Marie Alexander,** President and CEO, *Quova*
- **Marc Benioff,** CEO, *SalesForce.com*
- **Sandy Berger,** Former White House National Security Advisor
- **Jim Breyer,** Managing Partner, *Accel Partners*
- **Sergy Brin,** Founder, *Google*
- **Barbara Byrne,** Vice Chairman, *Lehman Brothers*
- **Marc Canter,** Founder and CEO, *Broadband Mechanics*
- **Mark Cuban,** Cofounder and Chairman, *HDNet and HDNet Movies, Owner of Dallas Mavericks*
- **Sky Dayton,** Founder and CEO, *Boingo Wireless*
- **Ned Desmond,** Executive Editor, *Times Inc. Interactive*
- **Tim Draper,** Founder, Managing Director, *Draper Fisher Jurvetson*
- **Esther Dyson,** Chairman, *Edventure Holdings, Inc.*
- **Elizabeth Economy,** Director, Asia Studies, Council on Foreign Relations
- **Don Evans,** Secretary of Commerce
- **Jonathan Feiber,** General Partner, Mohr, *Davidow Ventures*
- **Bambi Fancisco,** Columnist, *Marketwatch*
- **Alice Gast,** VP for Research and Associate Provost, *MIT*
- **George Gilder,** Editor, *Gilder Technology Report*
- **Dan Gillmor,** Founder, *Grassroots Media Inc.*
- **Rob Glaser,** Founder and Ceo, *RealNetworks*
- **Jordan Greenhall,** Founder and CEO, *DivX*
- **Trip Hawkins,** Chairman and CEO, *Digital Chocolate*
- **Mike Homer,** Cairman and Cofounder, *Kontiki*
- **Paul Jacobs,** CEO, *Qualcomm*
- **Bill Joy,** Managing Director, *Kleiner Perkins Caufield & Byers*
- **Rich Karlgaard,** Publisher, *Forbes*
- **Guy Kawasaki,** CEO and Managing Director, *Garage Technology Ventures*
- **David Kelley,** Founder and Chairman, Ideo, and Professor of Mechanical Engineering, *Stanford University*
- **Joe Kraus,** Cofounder and CEO, *JotSpot*
- **Mark Kvamme,** Partner, *Sequoia Capital*
- **Jaron Lanier,** Visiting Scientist at *Silicon Graphics*
- **Larry Lessig,** Professor, *Stanford Law School*
- **Roger McNamee,** Cofounder, *Elevation Partners*
- **Marten Mickos,** CEO, *MySQL*
- **Jonathan Miller,** CEO, *AOL*
- **Steven Mills,** SVP, Software Group and Group Executive, *IBM*
- **Michael Moe,** Chairman and CEO, *ThinkEquity Partners, LLC.*
- **Allen Morgan,** Managing Director, *Mayfield*
- **Zach Nelson,** President and CEO, *NetSuite*
- **Curt Nichols,** VP, Intel Capital, and Director, Digital Home Sector, *Intel Capital*
- **Anthony Noto,** Managing Director, Internet & Entertainment Research, *Goldman Sachs*
- **Larry Page,** Founder, *Google*
- **Jim Plummer,** Dean of the School of Engineering, *Stanford University*
- **Kim Polese,** CEO, *SpikeSource*
- **Michael Powell,** FCC Chairman
- **Janice Roberts,** Managing Director, *Mayfield*
- **Joe Schoendorf,** Partner, *Accel Partners*
- **Jonathan Schwartz,** President and COO, *Sun Microsystems*
- **John Schwarz,** President and COO, *Symantec*
- **Stratton Sclavos,** CEO, *VeriSign*
- **Doc Searls,** Senior Editor, *Linux Journal*
- **David Sifry,** Founder and CEO, *Technorati*
- **Jayshree Ullal,** SVP & GM, Optical Networking Group, *Cisco*
- **Padmasree Warrior,** CTO, *Motorola*
- **Michael Weiss,** CEO, *StremCast Networks*
- **Ken Wilcox,** President and CEO, *SVB Financial Group and Silicon Valley Bank*
- **Niklas Zennström,** CEO, *Skype*

REGISTER NOW AT HTTP://WWW.ALWAYSON-NETWORK.COM

AlwaysOn
the insiders' network

Technology Review
AN MIT ENTERPRISE

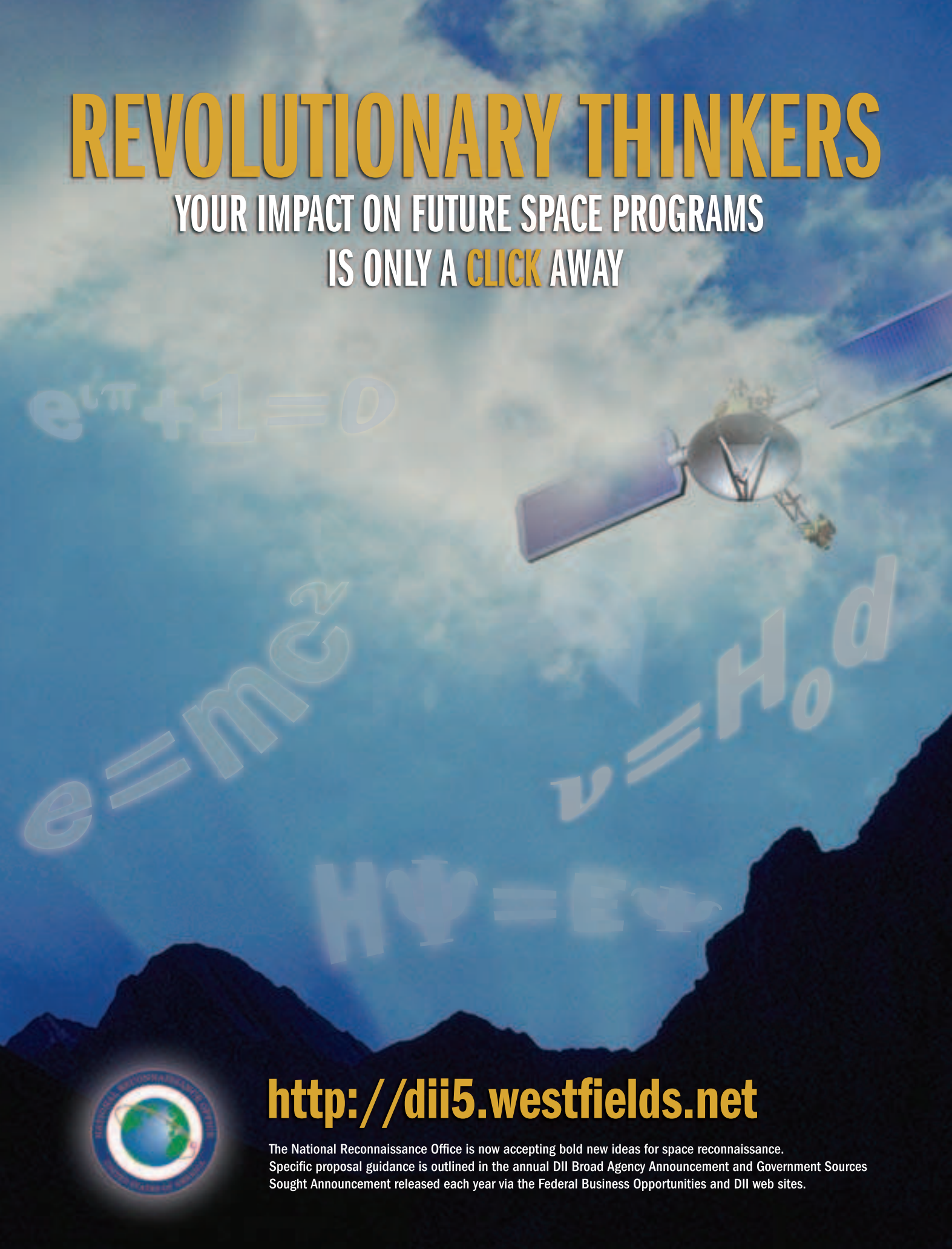
Customer Service and Subscription Enquiries

National: 800-877-5230
International: 386-447-6352
www.technologyreview.com/customerservice
Permissions: 978-750-8400
Reprints: 717-399-1900 x118
MIT Records: 617-253-8270 (alums only)

Technology Review
One Main Street, 7th Floor
Cambridge MA 02142
Tel: 617-475-8000
Fax: 617-475-8043

De Technologia non multum scimus. Scimus autem, quid nobis placeat.

Technology Review, the oldest technology magazine in the world, is published by Technology Review, Inc., an independent media company owned by the Massachusetts Institute of Technology. Founded in 1899, *Technology Review* describes emerging technologies and analyzes their commercial, economic, social, and political impact for an audience of senior executives, researchers, financiers, and policymakers, as well as for the MIT alumni. In addition, Technology Review, Inc. produces technologyreview.com, a website that offers daily news and opinion on emerging technologies. It also produces live events such as the Emerging Technologies Conference. The views expressed in *Technology Review* are not necessarily those of MIT.


REVOLUTIONARY THINKERS
YOUR IMPACT ON FUTURE SPACE PROGRAMS
IS ONLY A CLICK AWAY
http://dii5.westfields.net
The National Reconnaissance Office is now accepting bold new ideas for space reconnaissance.
Specific proposal guidance is outlined in the annual DII Broad Agency Announcement and Government Sources
Sought Announcement released each year via the Federal Business Opportunities and DII web sites.

Letters

The State of Bioweapons

Mark Williams's piece on the dangers of biotechnology is an excellent summary of the current tensions ("The Knowledge," March/April 2006).

Today's scientists have the responsibility to consider the possible abuse of biotechnological advance for hostile purposes, but they need not reinvent the wheel. In my 2005 book, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*, I analyze the different historical restraints that have prevented the use of biological weapons despite nearly a century of available technology and development. Why the large state programs, with the exception of the Japanese from 1940 to 1943, refrained from using germ weapons is a deep subject. I agree with Williams that the threat of advances in this area of science is real and that scientists need to be more aware of potential dangers, as well as threats to openness in research. The multiple layers of secrecy surrounding the state programs of the last century (and some in this century) increased risks to civilians. What members of the public do not know can hurt them.

Jeanne Guillemin
Senior fellow
MIT Security Studies Program
Cambridge, MA

You conclude your excellent explanation of why you decided to publish "The Knowledge" by stating, "Our best hope of countering the threat is to invest in research that will suggest a technological solution" ("From the Editor," March/April 2006). I could not disagree more. We are surrounded by serious problems for which technological solutions exist but are not employed. One needs only to consider how our dependence on petroleum might be reduced simply by raising the fuel efficiency standards for automobiles. Our best hope of countering the threat of bioweapons is to invest in research that will suggest a *social* solution.

David Nasatir
Berkeley, CA

In her essay about the cover story [for more on this, see next page], MIT's Allison Macfarlane doesn't rebut Williams's piece so much as point out that there are uncertainties about the ability of terrorist groups to create and to weaponize biological agents, as well as huge uncertainty about their lethality ("Notebooks," March/April 2006). I agree with this. But think of the problem this way: suppose one were to ask, What is the probability that a terrorist group could marshal the resources to design and build large jet aircraft for the purpose of suicide bombing? Wrong question. Terrorists are more likely to procure materials from state laboratories than they are to synthesize, say, smallpox by themselves. (This was true of the way the Soviets obtained atomic weapons and the Chinese acquired missile technology.) Therefore the big question is, What kind of bioweapons work is going on in the advanced nations?

Allan Dobbins
Birmingham, AL

Williams writes that even if we enacted George Church's proposal to register all DNA synthesizers and force certain classes of researchers to work transparently, "not all nations would comply. For instance, Russian biologists, some of whom are known to have worked at Biopreparat, have reportedly trained molecular-biology students at the Pasteur Institute in Tehran." It is important to note that educating students in molecular biology is by no means a violation of the Biological Weapons Convention (BWC) by itself. Moreover, even though the Soviet Union violated the BWC by developing bioweapons on its own territory, there has never been any known transfer of pathogens or weapons technology to third parties. Thus we have no reason to claim that Russia is a suspect country. Today, Russia is an active member of the BWC, and it renounced any bioweapons development activities in 1992. The problem of noncompliance is a very important one and is a major obstacle in the way of international implementation of the control mechanisms, but most experts would agree that this threat is not coming from Russia.

Aleksandr Rabodzey
Cambridge, MA

There is a short-term risk that, as we get up to speed with biotechnologies, we'll make honest mistakes, and a perpetual chance the technology will be abused. But it's important to keep in mind that for every person who would choose to do something destructive, there are tens of thousands that would do something more economically or personally satisfying. These technologies will accelerate life science capability across the board, creating a rising tide unlike anything seen since the early 1970s, when recombinant DNA tools materialized. Back then, we also feared the unknown. Despite doomsayers, we pushed ahead and never looked back. We didn't destroy the world with gene splicing, but we did change our understanding of biology for the better and made advanced diagnostics and therapeutics that help millions.

Andrew Hessel
Toronto, Ontario

Correction

In "The Knowledge," the cover story of our March/April 2006 issue, we mistakenly called the varicella-zoster (chickenpox) virus a poxvirus. It is a herpesvirus.

How to contact us

E-mail letters@technologyreview.com
Write *Technology Review*, One Main Street, 7th Floor, Cambridge MA 02142
Fax 617-475-8043
Please include your address, telephone number, and e-mail address. Letters may be edited for both clarity and length.

In the March/April 2006 issue, we invited Allison M. Macfarlane, a research associate in the Science, Technology, and Global Security Working Group at MIT's Program in Science, Technology, and Society, to write an essay in reaction to our cover story. After the story was published, Serguei Popov, its main subject, wrote us a dissenting note of his own. Popov is a professor at the National Center for Biodefense and Infectious Diseases at George Mason University and spent nearly 20 years developing genetically engineered biological weapons for the Soviet Union. Here is Popov's letter.

I just cannot comprehend how denying the threat of biological weapons could help us change the situation for the better, as Allison Macfarlane implies. She writes that during World War II, Japanese attacks with plague on Chinese cities had limited effect. But by the use of a notoriously primitive technique, more than 200,000 Chinese were killed. Macfarlane further writes that germ "weaponization" is a difficult task; the 1979 anthrax accident in Sverdlovsk, Russia, she notes, killed only 66. What a conclusion! The spores, which escaped from a military facility, had been weaponized so effectively that a minuscule amount caused more than 300 deaths, according to unofficial accounts, without special dispersion means or careful consideration of environmental conditions. Instead of weaponization, the Rajneeshees cult chose a primitive and effective way to put down at least 750 people with *Salmonella typhimurium*. The reason that nobody died is because this pathogen rarely kills. Had *Salmonella typhi*, which causes typhoid fever, been used in the salad bars, people would almost certainly have died. Macfarlane should have also known that the Aum Shinrikyo attacks in Japan failed because the cult used a harmless vaccine variety of anthrax bacterium. This only confirms Williams's argument: knowledge is a critical factor. So how difficult would it be for terrorists to acquire weaponization secrets? Anthrax letter attacks show that for some terrorists, the technology is not a hurdle. Have SARS, HIV, and the flu had to be weaponized in order to cause pandemics? Mark Williams asks another question: what if such viruses were reëngineered to become even more dangerous? I think we all know the answer.

Serguei Popov

Allison Macfarlane responds:
The issue is not how awful particular pathogens can be; surely this is well known. The issue is that biological weapons are now considered "weapons of mass destruction" in the mainstream media and in documents such as the Nuclear Posture Review, which states that if attacked with such weapons, the United States may respond with nuclear weapons. If the U.S. were to suffer an attack similar to the anthrax attacks of 2001, or even one in which hundreds died, would this justify the use of nuclear weapons?

Is it reasonable to include biological and chemical weapons in the same category as nuclear weapons, when our predictions of bioweapons capabilities are based on incomplete data sets?

One result of equating nuclear, biological, and chemical weapons under the category "weapons of mass destruction" is that funding for defense against these weapons is out of proportion to the threats. In fiscal year 2005, the federal government's request for biodefense spending was $7.6 billion. In comparison, U.S. spending for protection against the use of nuclear weapons on the U.S. (largely by securing former Soviet nuclear weapons and materials) was less than $2 billion.

As Professor Popov says, what's important is the knowledge. And in the case of U.S. policy, there is a lack of knowledge that informs the equating of nuclear and biological weapons. This could prove fatal one day.

How paper from Oberkirch reaches the four corners of the globe. Without interruption.

The Koehler Group in Oberkirch, Germany is one of the world's largest makers of specialty paper, used to make everything from airline tickets to Pokémon cards. Managing their output takes continuous 24/7 production—and HP Integrity servers with Intel® Itanium®2 processors. "We produce and ship over 1,500 tons of paper each day. A moment of downtime means production must stop," says Bruno O. Schwelling, CFO. "Itanium-based HP Integrity systems have virtually eliminated that fear." itanium-integrity.com

ITANIUM + INTEGRITY. ON AND ON AND ON.

intel hp invent

From the Editor

Rootkits Cross the Line

When a company trespasses upon its customers' privacy, it should expect outrage.

MARK OSTOW

Last year, anonymous executives at Sony BMG Music Entertainment blundered. They hid a "rootkit" on around two million compact discs.

As senior editor Wade Roush explains in this month's cover story, "Inside the Spyware Scandal" *(p. 48)*, rootkits are a kind of software more often exploited by mischievous hackers than by multinational media companies: a rootkit is capable of exposing an operating system's core functions to worms, viruses, or other programs, without anyone knowing about the subterfuge. In this case, computer users were asked to launch a Sony music player when they tried to play a Sony CD; if they did, they unwittingly downloaded a rootkit intended to hide components of a digital rights management (DRM) program. The DRM program also secretly contacted Sony every time a user played copy-protected music.

Sony's executives thought they were within their rights: they wanted to discourage piracy. But when security experts discovered the rootkit and blogged about it, a scandal followed. Many computer users said they felt "violated." According to John Guarino, the computer consultant who first identified the rootkit, "It's total lawlessness, and it's unacceptable."

Why were computer users so angry? In explaining themselves, most seemed to fret about trespasses upon their private property. But the complaints were much more heated than any damage to users' computers warranted (until Sony provided an uninstall program, removing the rootkit disabled users' CD-ROM drives). Sony's customers felt that the company had abused an interest related to property but distinct: they thought their privacy had been invaded.

The ambiguity of their complaints should not surprise. Privacy resists easy description. Philosophers or jurists eager to champion privacy as a coherent interest have nonetheless struggled to define it; others, less friendly to the idea, have argued that any interest we might protect as private can be more usefully defended by appeal to other interests, such as property, without the inconvenience of creating a new right or providing a cloak for illicit behavior. And certainly, people use "privacy" to describe very various interests.

This general confusion about what constitutes privacy has been much exploited by companies and governments in recent years. Indeed, as Sony's rootkit makes clear, much of our behavior in digital space is now potentially subject to observation, data collection, and coercion.

Yet privacy is real. There is a distinctive characteristic to *all* private experiences, although no *one* thing can be said to define privacy. But most of us recognize privacy when we experience it. Privacy is the space where we are free from interference. It is the necessary condition for intimacy, trust, and all contracts, including citizenship. And while the territory claimed for privacy will vary according to culture or historical circumstance, most feel aggrieved when we feel that territory shrink.

Sony's rootkit was *not* a trivial irritation, of importance only to geeks. The harm computer users suffered was limited (perhaps because the rootkit was discovered), but the offense was actual and new. Sony's customers objected on a point of principle: they believed they saw the chill expansion of corporate interests at the expense of privacy. They were right. **Jason Pontin**

Spain: Leader in Infrastructure Development

By Cynthia Graber

In the world of concessions for infrastructure development, Spanish companies lead the international market. Six of the 10 top transportation concession companies are based in Spain, constructing and/or managing about 40 percent of all major transportation concessions in the world. Spanish companies are taking their knowledge and experience into an increasing number of markets each year. This is the third in an eight-part series highlighting new technologies in Spain and is produced by Technology Review, Inc.'s custom-publishing division in partnership with the Trade Commission of Spain.

According to Greek mythology, when the shadowy souls of the recently departed made their way to the shore of the river Styx, they faced Charon, the one with the power to transport them to the world beyond. If the soul paid a toll, Charon ferried it across. If not, it wandered between death and life for eternity.

This use of tolls so vividly described by the ancient Greeks has roots in the real world as well. Historians note the use of tolls in the ancient Middle East and Asia, and England charged tolls for roads and bridges in the Middle Ages. In Spain more than a century ago, there are numerous examples of the crown authorizing a private individual to develop a public work such as a bridge or a wharf and recuperating the costs from individuals using the service.

Since the advent of the automobile, however, many governments in both developed and developing countries have assumed the responsibility for public spaces such as roads. Tolls have persisted, but most of these have remained in the hands of local or national authorities.

Today, there is a move afoot for private companies to run, manage, even at times to own what are primarily public spaces.

These are often done through Public Private Partnerships, and these models provide a method for governments to obtain much needed funds and for businesses to develop and invest in equally needed public infrastructure.

At the same time, advances in technology have allowed for a growing public acceptance of an increase in toll roads. The advent of electronic tolls, and even barrier-free toll roads, has created an ease of use that is contributing to the growth in tolls as a form of revenue for both public and private developers.

Due to the history of road development in Spain and the strength and experience of Spanish companies, these companies have assumed the lead in the global market for infrastructure concessions.

Why Spain?

The Spanish Civil War at the end of the 1930s left the country extremely poor, a situation that persisted for decades. In the 1960s, the government realized that building infrastructure such as roads was crucial for tourism and for the development of the country.

"At the time, we could only use peseta [the Spanish currency before the Euro] loans for investment, and peseta loans were limited to the accumulation of taxes," says Fernando Gutierrez de Vera, chairman of the concessions commission for SEOPAN, the major association of Spanish contractors. "But Spaniards were very poor with a very low income per capita. So this meant that there was not enough money in the system to be invested into the country's development."

In response, the government authorized the companies that would become the concessionaires to dip into the pockets of partners in richer countries. Those foreign loans provided the capital for the toll roads, with a backing from the Spanish government assuring a return on the investment if the toll income did not meet expectations.

"At the time, it was a daring decision, but it ended up working out very well," says Gutierrez. "The roads were paid off from the tolls themselves, and this contributed a great deal to the development of the country."

The process of using toll roads to build infrastructure began in the 1960s and 1970s, not only in Spain, but in other Mediterranean countries as well. Unlike Spain, however, France and Italy chose the model of having state-owned companies develop the roads, as opposed to the primarily private Spanish model.

According to Nicolás Rubio, business development director of Cintra, a leading toll road operator, another factor contributed to the strength of Spanish companies in the world market. The government awarded the first road contracts at the end of the 1960s, which meant that the roads would be built and open to the public in the early 1970s—then in 1973, the oil crisis struck.

"If you look at traffic development on those roads at the time, it was a tough start," says Rubio. The government came to the construction companies and offered to buy back the shares. "We looked at this business as a long-term investment," he continues. "Today it may not be performing, but this was a 35-year contract." Companies held onto their roads, despite the oil crisis. When the crisis ended and the market improved, the roads provided a solid return on the companies' investments.

Says Rubio, "We were looking at the future, and we saw value. And somehow that spirit and that strategy shaped the industry in Spain."

The early years of concessions, and the strength of the Spanish construction market, left the companies with a great deal of capital and decades of experience in building and operating toll roads. This has placed them in a strong position to take a leading international role as the market grows in Spain and around the world.

The Workings of a Toll Road Concession

In theory, building and operating a toll road may seem like a rather straightforward venture: build a road, then operate a toll to recuperate the investment. In practice, however, these types of projects are significantly more complicated.

From a financial perspective, when a private company submits a bid for the construction and/or management of a new road, or the improvement and management of an existing road, predicting the future is a crucial component of determining the bidding price. The company must be able to ascertain what improvements are needed and how to provide the types of amenities, such as increased signage and road condition information, that will attract new users. Bidders also have created models to attempt to predict what the usage of the road will be and how long it will take to reach peak usage.

"These are incredibly complex algorithms to try to predict travel behavior," says William Reinhardt, publisher of *Public Works Financing*. "Each company uses fundamentally the same information, but I think it's much more refined for those with on-the-ground ownership and operating experience. If you own a toll road, you understand in incredible detail travel behavior and pavement life and all other various variables."

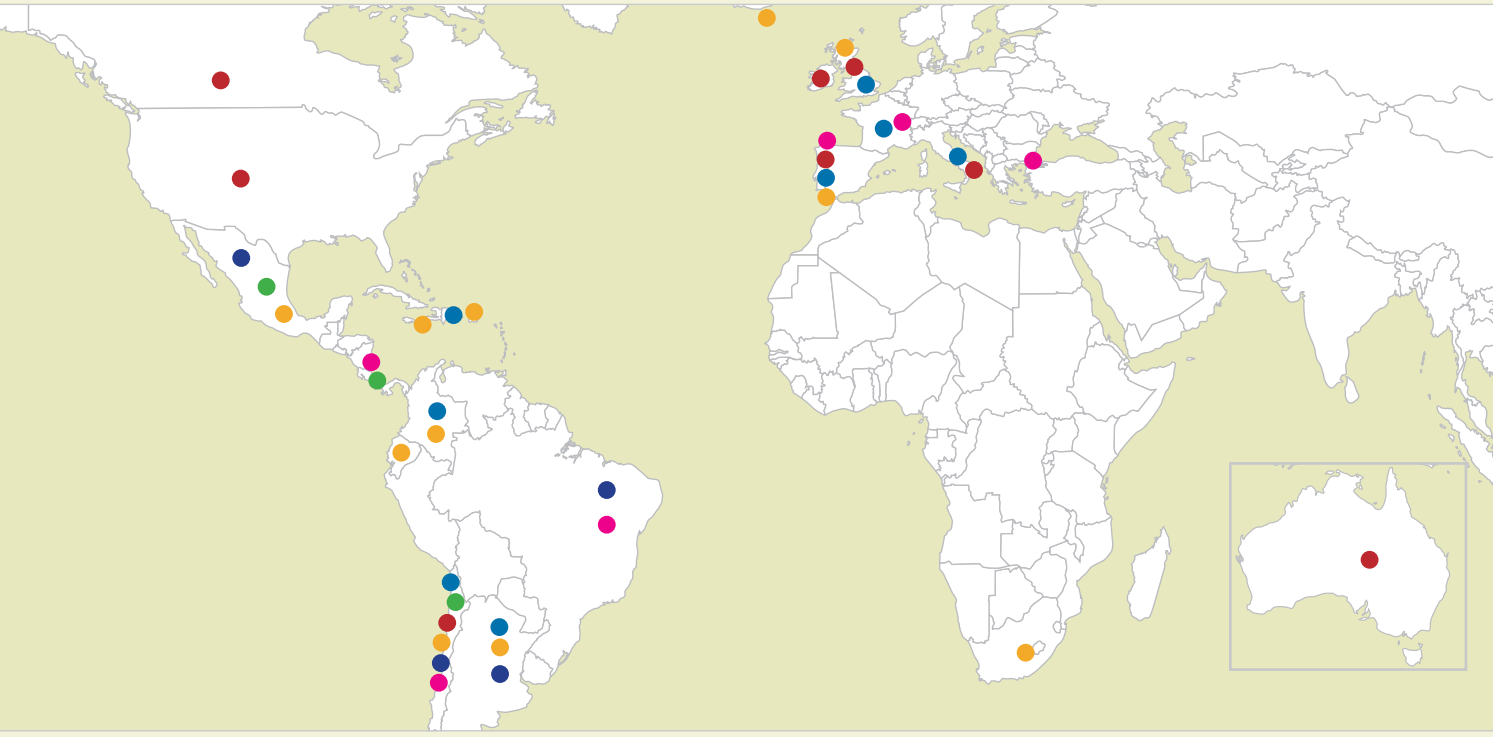
Managers have to negotiate the toll and toll increase potential with the local public authority. The private company expects a return on its investment while taking care not to raise the tolls so high as to push users to find alternative routes, while elected officials look to keep their constituency satisfied.

This relationship with the local authorities is crucial in terms of enforcement of nonpayment as well. Technological innovations allow companies to determine which drivers have paid and which haven't, but the regional authorities retain authority over fines for noncompliance.

Finally, the company must convince potential financial partners that an investment that will see no return for as much as a decade, and which may even register losses, makes good fiscal sense. "This is one of the most difficult elements to convey to potential partners," says Cintra's Rubio. "I think the innovation on our side has been to develop a way of proving to the market that it's a very good business, that entering into businesses that first generate accounting losses is a huge

Spanish Companies at the Top of the Global Market

Today, the international market is dominated by Spanish companies. In fact, of the top 10 toll road concession companies, six are Spanish: Grupo ACS, Ferrovial, Sacyr Vallehermoso, Abertis, FCC, and OHL. This map represents road concessions held outside Spain.



Abertis

Abertis is the largest operator in Spain, owning companies that manage more than half of the country's toll roads. Concessions make up 85 percent of Abertis's business, with 63 percent of the total business in roads alone. Internationally, Abertis has a strong presence in Latin America and is now expanding into the European market as well.

International Road Concessions: Argentina, Chile, Columbia, France, Italy, Portugal, Puerto Rico (U.S.), U.K.

FCC

FCC is a major construction and urban-services business, operating in more than a dozen countries. Its concessions business is concentrated primarily in Spain, with a handful of concessions located in Latin America. Though FCC is a major player in the concessions market, this is a relatively small sector of the company's overall business.

International Road Concessions: Chile, Costa Rica, Mexico

Ferrovial

Ferrovial is a major Spanish construction and services company, with operations around the world. Cintra, the name of the concessions company within Ferrovial, has currently taken the lead in the North American market. The company reported that in 2005, 64.5 percent of its concessions earnings were derived from its foreign concessions.

International Road Concessions (Cintra): Australia, Canada, Chile, Ireland, Italy, Portugal, U.K., U.S.

Grupo ACS/Dragados

Grupo ACS, a major construction and concessions company, is the largest concessions company in the world and has led the international ranking for the past 10 years. Concessions contributed 15 percent of the company's net profit in 2005.

International Road Concessions: Argentina, Chile, Colombia, Ecuador, Iceland, Ireland, Jamaica, Mexico, Portugal, Puerto Rico (U.S.), South Africa, U.K.

OHL

OHL is a major Spanish construction company with roots in the construction business stretching back to the early 1900s. In recent years, the company has been focusing increasingly on international contracts and currently operates in 16 countries. The concessions company, OHL Concesiones, has holdings primarily in Spain and Latin America, though goals are to expand into the European and North American markets.

International Road Concessions: Argentina, Brazil, Chile, Mexico

Sacyr Vallehermoso

Itinere, the concessions company within this global construction and real-estate company, contributes 30 percent of the company's earnings from concessions around the world. Through Itinere, Sacyr Vallehermoso is the largest motorway investor in Chile and operates 20 percent of road concessions in Spain.

International Road Concessions: Brazil, Bulgaria, Chile, Costa Rica, France, Portugal

opportunity." Their unusual approach, according to Rubio, involves creating worth through continually growing their business, adding new roads and projects, and holding on to the roads during the lean years with an eye to the long-term value and decreasing risk of the investment.

Spanish companies have thus far led in this sector because their years of experience have allowed them to develop successful models for predicting road improvements and usage, and to find creative ways to develop these complicated financial models.

According to Gutierrez, another reason the Spanish companies have been successful in the international market of road concessions, as opposed to straightforward construction, is that the main business of most of these large companies is difficult to export. On the other hand, the knowledge, skills, and financing experience are easily transferable when foreign markets open up tenders for concessions.

As it takes years, if not decades, to recoup the investment and begin seeing a significant return, the fact that Spanish companies are already seeing the maturation of some of the original investments places them in a strong financial position. Further, backing the concessions business are large construction companies with plenty of capital for investment.

Expanding Beyond Spain

As early as the 1970s, Spanish companies began building on their experience in Spain and capitalizing on a shared language to begin constructing and operating toll roads in Argentina, then moving onto Chile, Colombia, and Brazil. Recently this Latin American market has begun to grow, with Spanish companies as the primary foreign builders and operators. After a rough start and an unsuccessful period with toll roads in the early 1990s, due in part to poorly developed government financial models, Mexico is once again opening the country to toll road concessions. In 2003 OHL was awarded the bid to build and operate a 135-kilometer toll road that will allow drivers to avoid the entrance to Mexico City.

Though the Spanish market slowed in private road investment as later governments once again assumed the responsibility for road development, in the past decade this model is once again gaining importance in Spain and around Europe. In 1992, the 15 members of the European Union signed a commitment called the Maastricht Agreement, which strictly limits the annual deficit of each member country to three percent of the gross domestic product. Due to this, in Europe, governments can no longer greatly increase their debt to fund major public works.

In the U.K., the government coined the term "private finance initiative" (PFI) to refer to a private company developing a public infrastructure, in which users pay the company directly. The government has said repeatedly that this is not simply to reduce public debt but rather that private companies have proven to be more efficient and effective. Many examples of PFIs have been opening in the U.K. Across the water in neighboring Ireland, Cintra and Grupo ACS won toll concessions, and Grupo ACS is the top contender for another.

Abertis, the primary toll road operator within Spain, recently more than doubled the miles of their operations by purchasing Sanef, a French state company operating motorways in the north and east in the country. "That network in the north of France connects with Belgium, the Netherlands, the U.K., and Germany, and we think it's logical to try to explore future opportunities that may arise in those countries," says Toni Brunet, communication director at Abertis.

As the concessions model had already proven successful within Spain, in 2003 the Spanish government enacted a new law extending beyond toll roads to allow PFIs to build and manage all types of infrastructure, such as airports and ports.

Into North America

No Spanish companies were operating toll roads in North America in 1999 when Cintra, working in conjunction with Australia's Macquarie Bank, won the tender in 1999 for Toronto's Highway 407—a 99-year contract and the largest privatization in Canada's history. "This fundamentally relied on the reliability of Cintra's estimate, based on their experience, that the toll road still had far to go in terms of reaching its peak travel," said Reinhardt. "They could see how much it would cost to improve the roads. And incredibly boldly, they saw that there was a business in the United States that was going to evolve. So they bet heavily on the Toronto toll road, which included a major construction component and a number of other kinds of risks. They now turned this into a very profitable asset."

As part of the improvements to Highway 407, Cintra installed the first system of boothless tolls, called gantries, and invested in other improvements to increase ridership. This proved successful: within the first three years, the road quadrupled in appraised value.

Continues Reinhardt, "They've used the success of this very risky venture as a horse to ride through the U.S."

While the rest of the world began to embrace privately-funded toll roads, the U.S. has been significantly slower to open its doors to this type of investment.

Despite the fact that American citizens today may assume that the local, state, or federal government always retained authority over infrastructure, in fact the history of the U.S. mirrors that of the rest of the world in private infrastructure development. "Before railroads took the freight away, we had hundreds and hundreds of privately owned, privately chartered toll road companies all around America," says Peter Samuel, publisher of *Toll Roads News*. "But pavement couldn't compete with steel rail, and turnpikes fell by the wayside." By the Depression in the 1930s, nearly all private roads were under the ownership and operation of state authorities.

The state and federal authorities, however, are facing a challenge today in funding necessary improvements and new construction. In the U.S., highway funding has been provided by a gasoline tax,

Lights illuminate the Chicago Skyway, the first major toll road in the U.S. to be privatized, which is now operated by the Spanish company Cintra.

the proceeds of which are earmarked for transportation expenditures. This tax began in Oregon in 1918 and soon spread to all other states. Today, the states impose an average tax of 20 cents per gallon, while the federal tax is a little more than 18 cents. The federal government has not raised the gasoline tax in more than 20 years.

At the same time as the gas tax has remained steady, vehicles have become more fuel efficient. "It was a popular idea to fund the highways with what is basically a user fee. But now, for every mile you drive, you're using half as much fuel as in the past," says Martin Wachs, director of transportation, space, and technology with the Rand Corporation. Around the country, this has led to a lack of dedicated funds for roads.

"In the past 15 years," says Wachs, "there has been a reluctance to either impose new tolls or increase the gas tax."

In addition, the market mechanisms in the U.S. have until recently provided a challenging environment for private investment. Bonds issued by public authorities for the development of infrastructure are not subject to federal and state tax, meaning that "the cost of

public debt is less expensive than the cost of private debt," says Reinhardt.

Reinhardt explains that the way to get around this, and to assist private investment, is by the formation of something called a nonprofit public purpose corporation, which provides the legal framework for a public private partnership (PPP). Further, Congress's highway reauthorization bill of 2005 contained sections that extend this tax-exempt status to private companies funding toll road development. This provision allows companies to raise up to $15 billion through tax-exempt bonds for highway projects, a way of leveling the playing field.

States have also needed to change laws to allow for these PPPs in the management and operation of toll roads and other infrastructure systems; approximately 10 states have already changed their laws, and a handful of others are finding ways within the existing legal structure to allow for PPPs.

The combination of dwindling funds for roads, an awareness of the success of PPPs overseas, and the deliberate adjustment of tax and legal systems to allow for these new private initiatives has opened the doors to new, major toll roads—thus far dominated by one Spanish company, Cintra.

There are numerous examples of small, local toll roads built and managed by private companies, but the sale of the Chicago Skyway, the city's only toll road, for an unprecedented $1.83 billion in 2004 marked the first time an existing U.S. toll road had been sold. A partnership of Cintra and Macquarie Infrastructure Group purchased the rights to improve and operate the Skyway, a 12-kilometer stretch of elevated highway that reaches the border with Indiana, for the next 99 years.

The City of Chicago's windfall, and the success thus far of the concession, has piqued interest around the rest of the country in these high-stakes sales. Indiana received an offer of $3.85 billion from the Cintra partnership for a toll road crossing the state between Ohio and Chicago. This offer, for a 75-year concession, trumped the Chicago Skyway as the most money offered to a U.S. municipality for an asset. Cintra says it plans to spend about $700 million over the first nine years for electronic tolling and other improvements, and to add about 20 kilometers of new lanes.

Though Cintra won the bid, Spanish companies accounted for all four of the companies qualified to bid for the road.

Cementing its leadership position in the U.S. thus far, Cintra also was chosen as a strategic partner with the state of Texas for the development of the Trans-Texas Corridor. At first analysis of the needs of the planned corridor, Cintra has proposed developing at least five toll roads and investing approximately $6 billion.

Despite the apparent success of private toll roads and frequent municipal enthusiasm for the cash infusion, there have been examples of local opposition to private toll road concessions. Most in opposition decry the higher toll rates that will go into effect, and the idea of a private company—especially a foreign one—managing and making a profit off local infrastructure.

"People think they can use political influence to keep toll costs down if it's a state enterprise, but a private concession has a formula in which it allows regular toll increases on an annual or biannual basis," says Samuel. "They just think they'll be paying a lot more tolls, it's as simple as that."

Governments respond that tolls would need to rise in the near future, whether managed by a private company or a public authority.

There have also been security concerns expressed about toll roads, which are public assets, being owned or controlled by foreign companies. Experts, however, conclude that such concerns are unfounded, as local and state police departments remain in control of security.

As the experience of PPPs handling toll road concessions grows in North America, an increasing number of municipalities have expressed interest in reaping the benefits, and all major Spanish companies have plans to submit bids for future projects.

Technology

The significant growth of toll road concessions is in part due to technological advances of the past decade. "Tolling is now much more acceptable to the public. It's much less hassle, less onerous, you don't have to line up and wait," says Samuel, publisher of *Toll Road News*. "You can just buzz through. And now especially with open-road tolling over a normal section of highway, you don't even have to slow down."

"You can just buzz through. And now especially with open-road tolling over a normal section of highway, you don't even have to slow down."

Many drivers have recently come to appreciate the ease of new systems, where cars with a tag or transponder, connected to an account with a deficit or credit card, can sail through the toll barricades without stopping to hand over money. The next generation of toll roads, already in evidence on a handful of roads around the world, employ a system of what are called gantries, which hang over the road and read a vehicle's transponder. The gantries also capture other information such as a car's license plate number so those users without tags can be charged.

"The assurances have to be very high," says Reinhardt, publisher of *Public Financing Works*. "You have to provide the ability to take incredibly accurate video images of license plates, so the system will hold up in court. Also there's the issue of privacy and security. This has to be a fail-proof system. The banker wants to know that you can toll and identify everybody on the road." Privacy laws in some countries do not allow the use of gantries.

Cintra employed the first free-flowing toll road in the world in Canada, and today these systems have been developed in South Africa and Chile, where Spanish companies have employed them to great success.

Advances in imaging technology have allowed for collection of license plate information at high speeds. Laser scanners are employed to recognize the dimensions of the vehicle for classification and charges.

The development of gantries is based in large part on defense technology—the ability to detect and identify objects in the distance or determine friend from foe—and many of the top companies developing gantries have been involved in defense research. The systems work by employing a combination of imaging, radio frequency, and laser technology to read a car's transponder as it speeds by, and also to accurately identify vehicles without transponders. This last challenge has been the biggest one, but recent advances in imaging technology have allowed for the collection of license plate information at high speeds. Laser scanners are employed to recognize the dimensions of the vehicle for classification and free collection.

The Spanish company SICE has been able to take advantage of its long experience in the field and extensive knowledge of toll-road technology and present complete packages to interested companies. Grupo ACS used the gantry technology integrated by SICE in the first free-flow toll road in South Africa.

Telvent, another Spanish company, spends a significant portion of its revenue on R&D and has developed its own proprietary free-flow technology. In addition, Telvent is developing what's known as Sat-Toll, a system of open-road tolling based on satellite systems such as GPS or the European system Galileo. This is the most advanced form of tolling in the world, based on an onboard transponder that communicates the vehicle's position based on the satellite system. The location is then routed through a computer system that gauges the necessary tolls. Though no toll roads offer this system yet (it is being tested on trucks using highways in Germany and Australia), Telvent plans to be among a limited number of international companies marketing this new technology. "Thanks to our range of products, we're competing internationally in a large number of countries, on five continents, with the top companies," says José Montoya, Telvent general manager for traffic technology.

These toll-road technology companies have also developed the information systems necessary for real-time processing of the information collected and the database systems necessary for the management of that information.

Charging models for tolls vary: some toll roads charge different amounts based on the time of day (higher for high-traffic periods), while others may develop specific toll lanes that will provide faster access for those willing to pay a premium. Innovations in technology and financing have contributed to the success of all these models.

Another technological challenge facing those developing the latest toll road technology and software is how to coordinate between different and potentially incompatible systems of electronic tolling.

Tecsidel, a Spanish information systems company, dedicates a significant segment of its operations to traffic and tolling. Their main product is the software that integrates a wide range of traffic information, including real-time signals from road sensors that must be processed quickly. This information goes to a central software system that manages large databases.

Tecsidel recently won a bid to design and deliver a system in Norway that can recognize and integrate different tagging standards: Norwegian, Swedish, Danish, and the general European standard. There are different communication protocols for tags of different standards, and any interoperable system must also be able to communicate with and charge the different clearing centers.

The company's current R&D involves using laser systems to classify automatically vehicles within a variety of parameters, such as the length, height, and width of the vehicle, and the number of axels.

Indra, a major international Spanish

company heavily involved with defense information research, also devotes significant resources to traffic and transportation. The company uses their intelligent systems in conjunction with a wide variety of technology to provide all systems of tolls.

Many of these companies, including another Spanish firm, Etra, use similar information technology to provide world-class intelligent transportation systems, a computer-based system that optimizes the movement of urban traffic.

Technological innovations can be employed in more than tolling technology. "We were recently awarded a highway in the north of Italy," says Rubio of Cintra. "So we thought, how can we make it more attractive to users? We had an idea; this is an area with many foggy mornings. And there's a new system being developed whereby, every 50 meters, a special electric sign with lights and radar will tell you on foggy mornings what is the optimal speed to drive or if you have to stop, if there are cars stopped up ahead. So we built this into our proposal: it increased the investment, but it allowed us to imagine that we'll be able to attract additional cars."

Using their knowledge and experience to integrate all the available technologies from around the world allows companies to win bids. But, Rubio says, companies always have to be watching the market for new advances. "Nobody had proposed using that system," he says. "But once it's built, everybody bidding will put the same feature into future bids. So we have to look for new ideas. We always want to be one step ahead of the others."

The Future

Though governments control most airports on the European continent, airport privatization has slowly been gaining interest in Europe and around the world, and Spanish companies have used their experience in toll road privatization to take advantage of this trend as well. In addition, Spanish companies have holdings of ports, parking lots, even hospitals, all as part of the overall concessions portfolio.

When it comes to the growth of private toll roads, Samuel sees a number of places in the U.S. opening up to these types of projects. Says Samuel, "This is being studied in Houston for a road that could bring about $7 billion or $8 billion for the state. And I think New Jersey is also going to be a big one, because the finances are in a horrendous state, and they have such small amounts of money to service the debt of the transportation trust fund." Texas is home to a great deal of toll road excitement: many toll roads are in the planning or construction phase, and a number may well be developed as PPPs.

Samuel says that, around the country, "state toll authorities are heavily in debt and would need to raise their toll rates quite steeply in order to support new projects. They're loathe to do it as public authorities, and the thought is that it's easier to explain toll rate increases if the toll concessions are explicitly businesses."

Companies in this sector are closely watching the U.S. market. Though Cintra has already firmly established itself as a leader in the U.S., other Spanish toll road concessionaires operating overseas also hope to find a niche in North America.

In Europe, an increasing number of countries are turning to this model. Wealthier European countries are open to private financing to reduce public debt, while poorer Eastern European countries rely on the private market to invest in needed infrastructure development.

At the same time, companies flush with capital search for relatively stable, long-term investments. Toll road concessions have already proven to be one option in a diverse portfolio. And increasing advances in toll technology allow for greater accuracy and ease of use in the next generation of toll roads, those employing open road tolling.

Spanish companies, with their strong standing at the head of this international market and their extensive knowledge of the entire field, hope to continue to take the leading role in constructing and operating infrastructure concessions around the world.

Resources

ICEX (Spanish Institute for Foreign Trade)
www.us.spainbusiness.com

Abertis
www.abertis.com/en/

FCC
www.fcc.es/fcc/2003/ing/presentacion.htm

Ferrovial/Cintra
www.cintra.es/index.asp

Grupo ACS
www.grupoacs.com/eng/home.html

OHL Concesiones
www.ohlconcesiones.com

Sacyr Vallehermoso
www.gruposyv.com

SEOPAN (The Association of Spanish Contractors)
www.grupoexport.seopan.es

To find out more about New Technologies in Spain, visit:
www.technologyreview.com/spain/toll

For more information visit:
www.us.spainbusiness.com

Contact:
Mr. Enrique Alejo
Trade Commission of Spain
in Chicago
500 N. Michigan Ave., Suite 1500
Chicago, IL 60611, USA
T: 312 644 1154
F: 312 527 5531
chicago@mcx.es

ICEX
Spanish Institute for Foreign Trade

Forward

INFOTECH

Beaming Books

A cheap stopgap for the digital divide: satellite transmission

Eleven-year-old boys in Mbita, Kenya, view textbooks on handheld PCs last year.

COURTESY OF EDUVISION

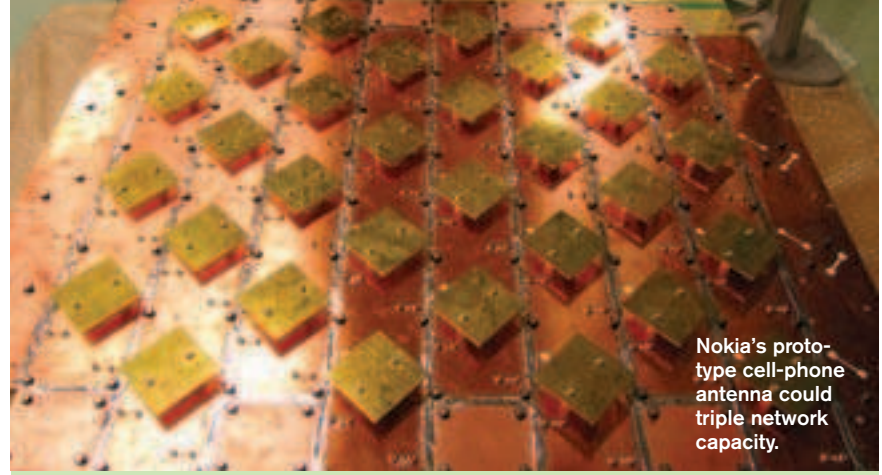
Many of Africa's cities and populous areas are reaping extraordinary benefits from new cellular telephone networks and Internet access. But it will be many years before rural interior areas—where the majority of Africans live—follow the cities into the information age. Children there don't even have recent-edition textbooks, much less Web-connected computers.

But help could be on the way in the form of a narrowband but workable technology: one-way delivery of digital information via satellite. In a test last year at the Mbita Point primary school on the Kenya-Uganda border, 60 youngsters got a taste of what's possible. A Swiss foundation called BioVision installed a satellite receiver at the school, gave out handheld computers running Linux-based software, and downloaded up-to-date curricula from Kenya's education ministry. BioVision says this approach is far cheaper than buying books every year.

Now, the foundation has passed the project, called EduVision, on to a venture capital firm called Bridgeworks, which hopes to turn it into a self-sustaining business. Bridgeworks is in talks with education agencies in several countries about implementing the system on a massive scale; a possible Rwandan project would serve more than 20,000 children in 504 secondary schools. "Our idea is that it will not be highly profitable but profitable enough to expand," says Matthew Herren, a Swiss raised in Kenya who started the project. He predicts that at least one of the countries now in talks will be using the system within a year. The satellite bandwidth comes from a Silver Spring, MD, company called WorldSpace, which operates two geostationary satellites, one over Asia, the other over Africa. For several years, the company has transmitted traditional satellite-radio content—audio feeds from outlets like CNN and NPR. Some African countries, including Kenya, have used the services to transmit audio versions of

classroom lectures. But in the past two years, WorldSpace has opened up some bandwidth for the broadcast of any digital information, delivered at 128 kilobits per second. That's slow by the standards of a Western office worker but sufficient to get text documents through quickly. Photos and videos mean longer wait times, but that's fine for the periodic downloading of educational materials. "One of the reasons why African educational systems have fallen behind, particularly in the sciences, is that it's very expensive to update and revise curricula," says Calestous Juma, an international-development professor at the Belfer Center for Science and International Affairs at Harvard University. Remarking on the isolation of Africa's interior, Juma added, "Africa has been waiting for something like this since the time of Julius Caesar."

While the system doesn't provide two-way communication, it can have a big impact on the delivery of educational, health, and agricultural information. In many regions, WorldSpace provides the only service that allows data download to cheap receivers with palm-sized antennas, as opposed to the expensive, high-bandwith satellite receivers used by governments, says WorldSpace senior vice president Srinivasan Rangarajan. **DAVID TALBOT**



Nokia's prototype cell-phone antenna could triple network capacity.

TELECOM

A Cell-Phone Tower with Focus

When you talk on a cellular phone, you're sharing radio frequencies with everyone else within a three-kilometer radius of the nearest base station. Congestion can lead to static, dropped calls, and slow downloads. In the basement of Nokia Research Center in Helsinki, Finland, Nokia has forged a new kind of antenna that focuses signals where most needed and could increase network capacity threefold.

A traditional cell-phone tower works like a lawn sprinkler that radiates in all directions. Nokia's antenna works like a hose. It's fashioned out of copper strips, each about eight centimeters wide, welded together into a surface covering about one square meter. A case behind the copper sheet contains sophisticated amplifiers and digital signal-processing circuits that steer as many as eight separate beams in different directions, depending on demand. "The basic idea is that in a crowded area, you want to give the maximum signal to the appropriate person rather than wasting the energy by spreading it out over a broader volume," explains Greg Hindman, president and cofounder of Torrance, CA–based Nearfield Systems, which builds testing and measurement systems.

While the antenna could theoretically increase network capacity by a factor of eight, geographical obstacles and other sources of interference mean it actually doubles or triples capacity, says Hannu Kauppinen, senior research manager for radio technologies at the research center.

Nokia is not alone: many telecom researchers are working on ways to increase the capacity of the newest generation of cellular networks, called wideband code-division multiple-access, or WCDMA, systems. **WADE ROUSH**

SOFTWARE

Smart Cameras

New tool deciphers text in video

Government and private surveillance companies have a new weapon. Software developed at SRI International in Menlo Park, CA, can identify words and numbers in moving video taken under difficult conditions. The software locates characters, extracts them from the background, and adjusts for lighting or angled views. Gregory Myers, program director at SRI, says the software could be used in applications ranging from video archiving to homeland security. The software works by examining each frame of a video for sharp lines set against a contrasting background—telltale indicators of character strokes. Since text often persists over many frames, the software also looks for text similarity among frames to increase accuracy. If characters are warped or unclear, image-processing algorithms straighten them and even out their tone. The cleaned-up characters are then fed into optical character-recognition engines that convert them to machine-searchable text. The company is working with government agencies that need to identify ships and vehicles from rough video; Myers expects that the software will soon be available for private consumer use as well. KATE GREENE

New software extracts letters and numbers from video taken of a pickup truck.

COURTESY OF NOKIA (CELL PHONES); COURTESY OF SRI INTERNATIONAL (CAMERA)

MEDICINE

Implantable Medication

Programmable drug chips pass longevity milestone

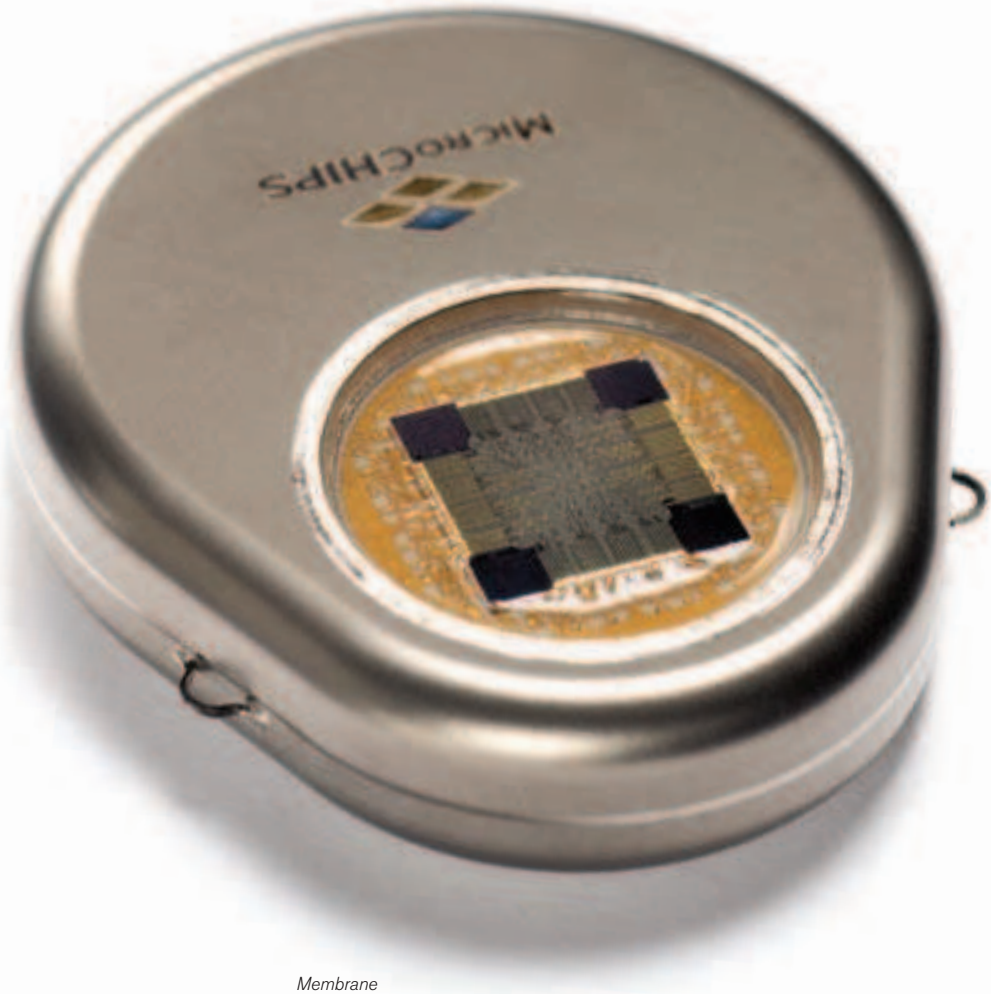
Implantable devices being developed by a Bedford, MA, company called MicroChips may one day replace the tedious ritual of regular drug injections. Instead, doctors could program a chip under the skin, allowing drug doses to be released on schedule from any of 100 microscale drug reservoirs.

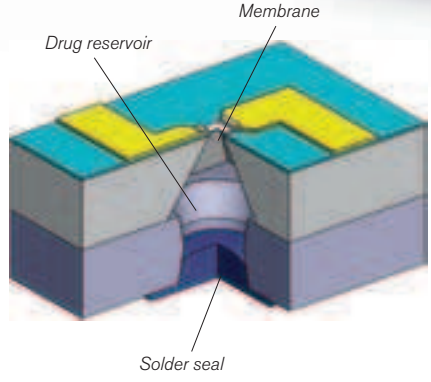
The company took its first step toward proving such a device is possible in March, when results of the first animal test of an implantable drug-delivery system were published. MicroChips scientists showed that such devices stably released a biological drug in dogs for up to six months—an unprecedented feat.

About the size of an Oreo cookie, the device used in the test consists of a silicon and glass microchip that contains 100 miniature drug reservoirs, each about 50 micrometers wide at the top, plus a battery and electronics controlling drug release, sealed in a titanium case.

Such a device would have obvious benefits for diabetics but could also provide a sophisticated delivery method for almost any type of drug. "This is a major step forward in drug delivery," says Henry Brem, director of neurosurgery at Johns Hopkins University School of Medicine.

Brem highlights brain and spinal tumors as an area that might particularly benefit. He hopes that such a device might be useful in his own efforts to create a tumor vaccine for brain cancer patients. A microchip could release steroids, to control brain swelling, as well as a standard course of targeted chemotherapy drugs directly into patients' brains after a single surgery.





Key to the implantable MicroChips device (top) are 100 pyramid-shaped drug reservoirs (bottom) about 50 micrometers wide at the top. A wireless signal from outside the body prompts the device to melt a thin metal membrane covering a specific reservoir, releasing a drug directly into human tissue. A solder seal holds the drug in place.

The device tested in dogs was activated wirelessly, and is poised for further improvements. John Santini, cofounder and president of MicroChips, says that before human tests are launched, the device will be further miniaturized—to about the size of two stacked 50-cent pieces—and built to last at least one year. Like the tested device, it will be programmable, so external activation of the drug reservoirs won't always be required.

The company plans to use the same basic design to create long-term, implantable sensors to monitor blood sugar levels in diabetics. Such sensors could also trigger drug release. MicroChips hopes to test these sensors in people within three years; a drug delivery device might reach human trials within five years. **ERIKA JONIETZ**

PHOTO BY CHRISTOPHER HARTING; GRAPHIC COURTESY OF MICROCHIPS

INTELLECTUAL PROPERTY

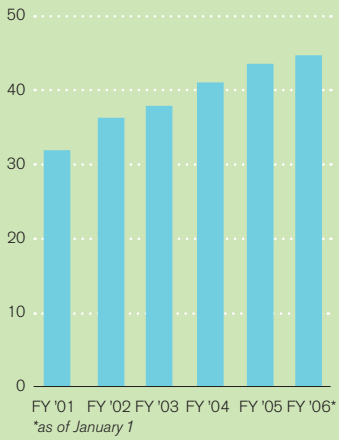
Patent Pileup Worsens

The backlog at the U.S. Patent and Trademark Office keeps breaking records. And if you want to know the pain that it causes, just ask venture capitalist Greg Blonder. Blonder, a partner at Menlo Park, CA–based Morgenthaler Ventures who specializes in software and nanotechnology, says two promising companies he has worked with were nearly sunk by the sluggishness of the patent office. "Not only couldn't we find investors because we couldn't establish our clear rights to the technology," Blonder says, "we ended up having to spend more than a million dollars to litigate in patent cases that could have been avoided."

Last year, in Senate testimony, Jon Dudas, under secretary of commerce for intellectual property, bemoaned a patent backlog of "historic proportions." Since then, things have only gotten worse. The problem is due in part to the growing length and complexity of patent applications. Today, with some 600,000 patents in the queue, applicants in high-tech areas like software will wait nearly four years before knowing whether their patents have been granted. Given the pace of technological change, it is little wonder that even attorneys are starting to lament what Michael K. Kirk, director of the American Intellectual Property Law Association, calls "a cloud of uncertainty over the marketplace."

Want a Patent? Get in Line

Months taken for decisions on computer architecture, software, and information security patents

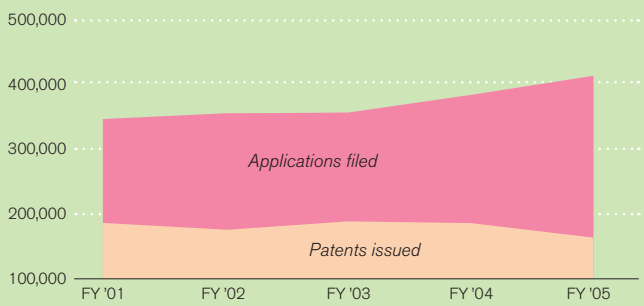


Federal officials are pledging to hire as many as 1,000 new patent examiners this year, but given the scale of the bottleneck, expert analysts say it could take close to a decade to fix the problem. The worst part, says Blonder, "is that the problem is getting so bad it threatens to discourage entrepreneurs. At the end of the day, that's the last thing you want to do."

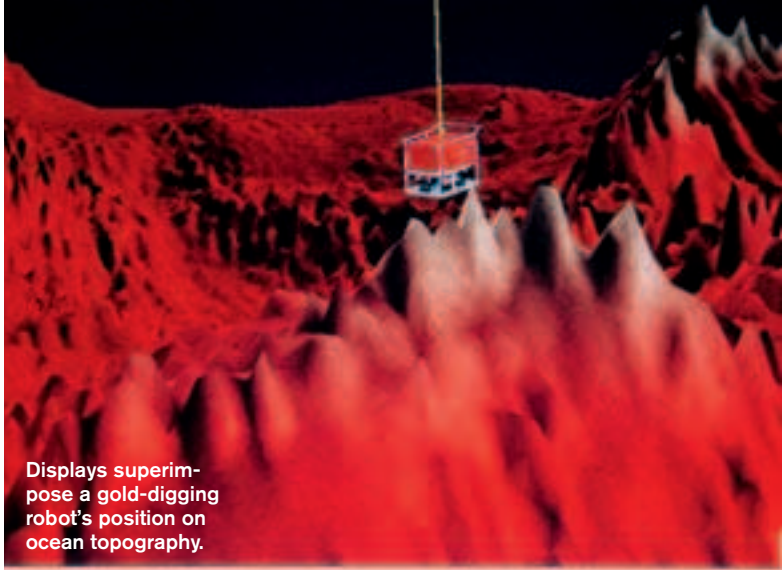
SETH SHULMAN

The Intellectual-Property Gap

Fewer patents are granted, even as application numbers grow



Source: U.S. Patent and Trademark Office



Displays superimpose a gold-digging robot's position on ocean topography.

ROBOTICS

Technology in the (Ocean) Trenches

Heavy-duty mining robots can now dig for gold in rocky, underwater landscapes at depths of as much as two kilometers. Earlier this year, a Canadian company, Nautilus Minerals, dispatched a specially designed underwater mining robot to conduct the world's first commercial deep-sea search for gold and copper, off the coast of Papua New Guinea in a mountainlike landscape 1,600 meters below sea level.

The feat was made possible through a marriage of advanced 3-D mapping technology and heavy-duty mining gear. Nautilus started with a deep-sea ROV (remotely operated vehicle) normally used by the oil and telecom industries; the company customized it by adding drilling and cutting tools hitherto used only on land.

Nautilus also equipped the ROV with a multibeam sonar device that maps the landscape in real time; software combined the device's reports with ROV location data to present a graphical display to an ROV pilot in a surface ship above the drilling site. Using the display, the pilot guided the ROV through the first mining operation in the cold, dark, and craggy underwater environment. "This software allows us to view the real-time location of our ROVs and ship in relation to the mapped features of the ocean floor," says Tim Searcy of Nautilus Minerals.

The company is evaluating its findings and preparing to follow up with a bus-sized, 750-horsepower ROV, and possibly a 1,000-horsepower model—which would be one of the world's largest ROVs—made by Perry Slingsby Systems, to do full-scale mining in the same area off Papua New Guinea, where sulfur vents on the ocean floor leave valuable mineral deposits.

PATRIC HADENIUS

COURTESY OF NAUTILUS MATERIALS

MICROFLUIDICS

Printing Press for Biosensors

Biologists have long sought a cheap way to simultaneously detect different types of biological molecules in a sample, such as the several malarial proteins that might be present in a patient's blood. One approach uses polymer tags with bar code–like lines that glow different colors when receptors on the tags bind to specific molecules. But making such tags on a large scale has been prohibitively expensive, as each extra bar line adds another step to the manufacturing process.

Now a group of MIT researchers has created a microfluidic printing press that can produce tiny particles in a single step. In addition to biotags, the method can turn out all kinds of shapes—from keys to cylinders to swirls—that could be used to make everything from microelectromechanical machines to optical devices, fabrics, and even the miniature stirring bars and valves used in microfluidics. "This is a beautiful piece of work for continuous synthesis of particles, with great flexibility in the shapes that can be produced," says Howard Stone, a professor of engineering at Harvard University.

The process, developed by an MIT group led by chemical engineer Patrick Doyle, begins with one or several closely spaced, parallel, 100-micrometer-scale streams of liquid. The liquids contain the polymers' precursors, some of which may be bound to proteins that can serve as receptors on a biotag. A flash of ultraviolet light projected through a stencil causes the polymers to solidify in specific shapes. The resulting particles can have several "stripes"—each created from a separate stream of fluid.

KATHERINE BOURZAC

A new microfluidic polymer "printer" can cheaply make 50-micrometer fluorescing bar-coded particles (left) or custom shapes (top and bottom) for other applications.

COURTESY OF DOYLE LABS (BIOSENSORS); COURTESY OF GE (PLASTIC)

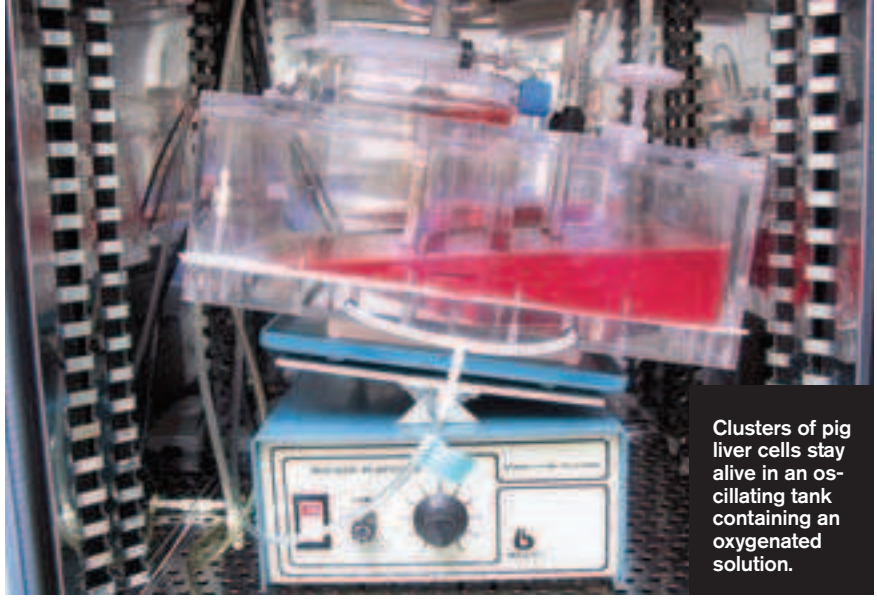
MATERIALS

Super Plastic

How would you like a self-washing car or a ketchup bottle whose contents flow freely? Researchers at General Electric have come up with a way to process a common polymer so that it repels fluid so effectively that even honey rolls right off it. The resulting property is called superhydrophobicity. While the property has long been achieved in expensive materials, GE's feat was to make it available in a common polycarbonate, Lexan. The discovery could allow everything from new, easy-to-clean building materials to cheap diagnostic devices with plastic microfluidic channels. In designing the material, GE took inspiration from the leaves of the lotus plant, whose surface cells are five to ten micrometers wide and topped by tiny wax crystals that are tens of nanometers wide. On a lotus leaf, water beads look like almost perfect spheres. GE mimicked this pattern on Lexan by "roughening" its surface in a similar way. Tao Deng, a materials scientist at GE, is tight lipped about the process but says it uses a "chemical treatment of the surface." GE estimates it will take at least five years to commercialize the technology, once all manufacturing issues are resolved.

DAVID TALBOT

A drop of blue-tinted water sits on nano-patterned superhydrophobic plastic.



Clusters of pig liver cells stay alive in an oscillating tank containing an oxygenated solution.

MEDICINE

A Lifesaving Liver Machine

With human liver tissue in critically short supply, the Mayo Clinic in Rochester, MN, is working to create a liver dialysis machine that uses pig liver cells. It's a step up from using whole pig livers for temporary treatment, because isolated cells present a lower risk of contamination and can stay alive longer.

Principal investigator Scott L. Nyberg tested his machine in late 2005 in a preclinical study on dogs with drug-induced liver failure. The dogs on the machine lived longer than control subjects and did not develop signs of brain swelling. "We want to extend the life span of the cells and duration of the treatment" compared to existing methods, Nyberg says. Some 40,000 Americans die of liver failure annually; Nyberg recalled a teenager who died 14 hours before a donor became available. "A device like this could have kept her alive just that one more day."

The device looks like a fish tank on a tilting platform. The tank holds an oxygenated liquid medium and about 500 grams of live liver cells, or hepatocytes, from pigs. The cells survive for up to a month when not in use and lasted 48 hours during the dog tests.

The blood of a liver patient would be filtered to remove white blood cells and immune proteins, so they can't attack the pig cells. The remainder would then mix with the hepatocytes for waste removal, pass through a membrane that blocks the pig cells, and reunite with the rest of the blood. Nyberg is preparing to do more animal tests; human trials could begin in 2008. **TOM MASHBERG**

WIRELESS

Cell Phones Say Hi to Wi-Fi

How'd you like just one phone number—and phone—for home, office, and mobile? Chicago-based BridgePort Networks officiated at the long-heralded marriage of cellular networks and Wi-Fi—which could mean cell phones that never drop calls inside buildings, where Wi-Fi is the cheaper and more reliable system.

At conferences in Barcelona and Las Vegas, BridgePort showcased new phones from Chinese manufacturer E28 that carry both a standard cellular radio and a Wi-Fi radio. When attendees wandered out of the Wi-Fi transmitter's range, the call switched to the cellular network. "They would never know when the handover was; there was no break in the pitch or the voice," boasts Todd Carothers, a BridgePort vice president.

Carothers called the conference events the first live demonstrations of call handovers using an emerging standard called voice call continuity, which bridges packet switching and cell switching. Companies such as Kineto Wireless in Milpitas, CA, are working on similar technologies, and business users can expect to see products by the end of this year. **WADE ROUSH**

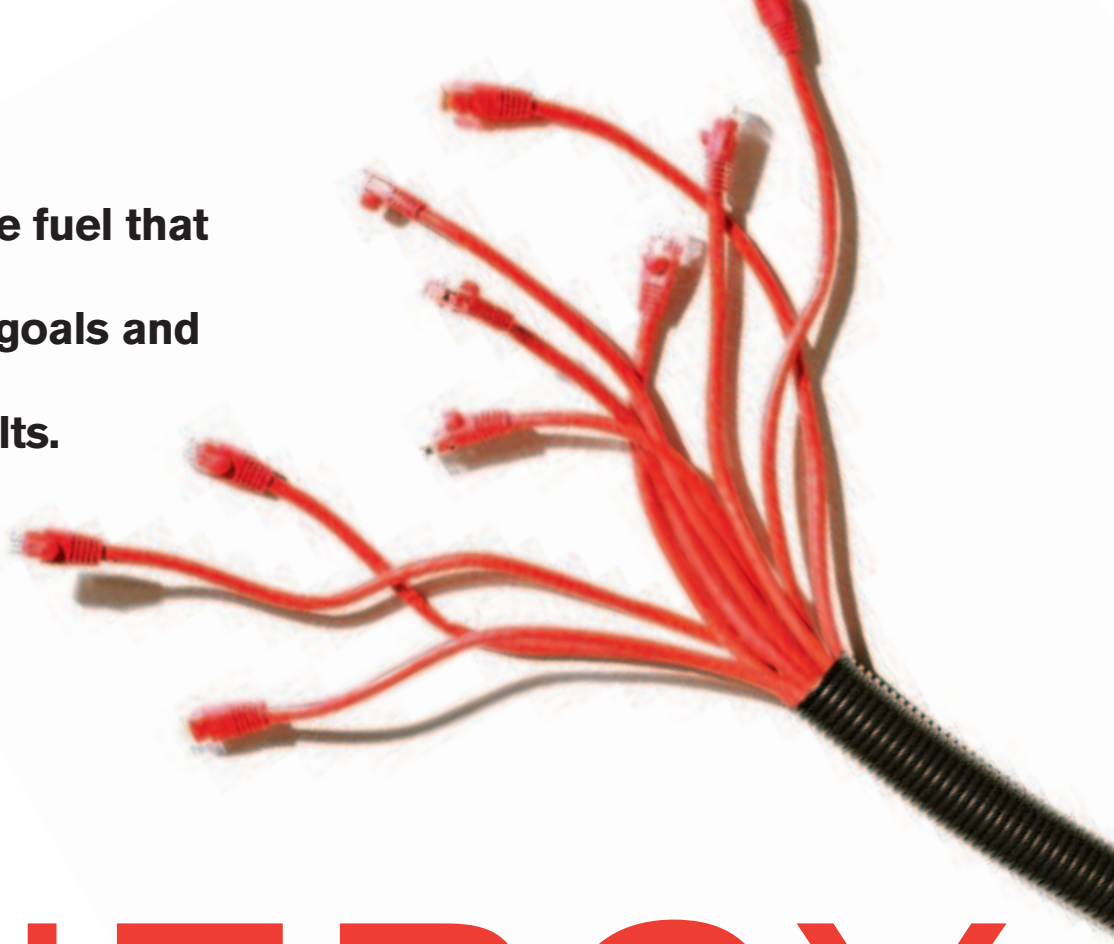
GAMING

Human Joystick

Video gaming is traditionally a sedentary pursuit, but that's changing thanks to interfaces that turn a player's motions into onscreen actions. Already, more than 1.5 million copies of Dance Dance Revolution, which challenges players to shimmy in sync with animated characters, have been sold; more than one million units of the EyeToy, a motion-tracking PlayStation camera that inserts players into games, have been sold through February. This year, Nintendo will introduce a game console whose controller contains a motion-tracking chip; in order to, say, thrust a sword in the game world, a player simply waves the controller in the air. And a startup called GameRunner has invented the first custom treadmill that controls off-the-shelf, first-person computer games. As the player walks, sensors underneath the belt translate its motion into in-game running or walking. The timing of such gadgets is good: "Everyone's concerned about childhood obesity," notes Joy Garner, cofounder of GameRunner. **DAVID KUSHNER**

COURTESY OF SCOTT NYBERG (LIVER); COURTESY OF GAMERUNNER (JOYSTICK)

Technology is the fuel that drives business goals and accelerates results.



ENERGY

When you're serious about intellectual property law for electrical, computer and Internet technologies . . .

Brinks attorneys are at the forefront of applying the intellectual property protections of patent, trademark and copyright law to emerging electrical, computer and Web technologies, as well as to business methods, domain name disputes, and many other issues related to the Internet. Brinks attorneys use their backgrounds and experience in electrical engineering, physics and computer science to counsel clients on the most effective intellectual property protection for their technologies. Brinks has the energy and resources to fulfill your company's intellectual property needs.

BRINKS HOFER GILSON & LIONE®

USEBRINKS℠
Intellectual Property Law Worldwide

866.222.0112
usebrinks.com

Q&A

RFID: At Risk from Viruses?

As part of an information system, even the lowly RFID tag is vulnerable

When Dutch researchers announced in March they'd managed to use radio frequency ID tags as a means of passing a virus to an information system's database, they merely demonstrated the obvious, says Daniel Engels, first research director at the Auto-ID Labs at MIT, a center of RFID research. RFID systems, being computers, are as vulnerable to viruses as any other computer. Good system designs and targeted applications minimize risk, Engels says.

***TR*: Generally, how vulnerable are RFID systems to fraud, attacks, and viruses?**

Engels: RFID systems, just like bar code systems, are computing and information systems. As such, they are potentially vulnerable. At the simplest level, think of a shoplifter who sticks a bar code for a 12-ounce jar of peanut butter over the bar code on a 16-ounce jar. He only pays the 12-ounce price, because that's what the information system is reading. The information system is relying upon the cashier to catch any discrepancies. An RFID tag could theoretically be switched, too.

How, exactly, are viruses a threat?

Most RFID tags are simple database devices. The data—commonly a product identifier plus a serial number—is either written in the wafer fab facility or at the point the tag is applied. Once data is written, it is locked, preventing any modification. You'd have to destroy the tag and replace it. Tags with rewritable memory may have a virus written to its memory, but the memory contents have no impact on the tag's operations. So most tags are not vulnerable to viruses, but some may be carriers of viruses.

What about the fancier tags?

Some RFID tags are able to store large quantities of data, such as the active tags used by the military to track its shipping containers. These act as unsecured databases and should be treated as such. Viruses may be stored in this user-memory portion. But the data typically needs to be in a specific format to be usable by the information system. This limits the potential for attacks, since incorrectly formatted data will be rejected by the system.

So it's up to the designers of the computing systems to stop such an attack?

As with all computing and information systems, security requires a multilayered approach when any automated identification system is used. RFID systems are simply an enabling technology. The power of the system lies within the information system using the captured data.

When RFID systems are used to store data other than the item's unique identifier, security measures must be used to authenticate the data and its authors. It is incumbent upon the information system to authenticate the data and verify that the format and structure of the data are appropriate for the applications using it.

What does the future hold?

As RFID technologies become more widespread and available at lower costs, the likelihood of various attacks will increase. But the potential security attacks on RFID systems and the information systems that support them are well known and well understood by experts within the industry. There is a price to be paid to implement countermeasures. As the cost and frequency of successful attacks increases, more security features will be integrated into the RFID tags themselves and the information systems supporting them.

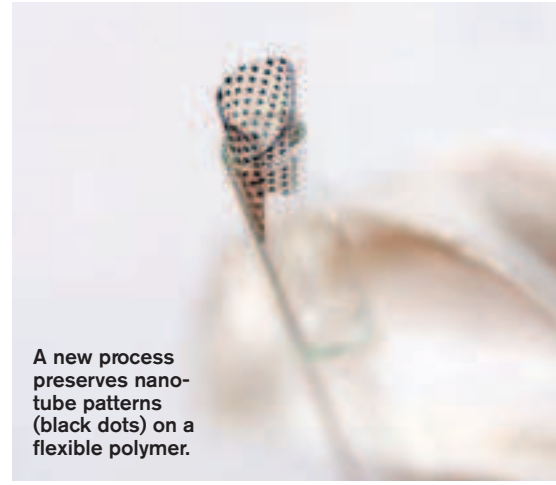
DAVID TALBOT

NANOTECH

Flexible Displays

Carbon nanotubes' unique electronic properties make them promising as, among other things, ultraefficient "electron emitters" for bright, low-power displays. Now, researchers have found a way to pattern nanotubes onto plastic sheets for flexible displays.

The new method, developed by researchers at Rensselaer Polytechnic Institute, Northeastern University, and New Mexico State University, starts with a surface prepatterned to specify where multiwalled nanotubes will grow on it. The researchers pour a liquid over the nanotubes and cook it until it forms a polymer. They then peel off the polymer and nanotubes. The polymer preserves the pattern right down to the positions of individual nanotubes, which it keeps aligned.



A new process preserves nanotube patterns (black dots) on a flexible polymer.

For displays, where single nanotubes must be isolated from others to get the best efficiencies, the researchers strip off a layer of polymer to expose the tips of nanotubes, then burn off long or tangled nanotubes, leaving isolated ones. "The results we've seen are some of the best that have been reported in the literature," says Swastik Kar, a postdoctoral researcher at RPI and a lead author of the paper. Prototype displays are still a few years off. KEVIN BULLIS

JASON SCHNEIDER (RFID); COURTESY OF YUNG JOON JUNG (DISPLAYS)

ROCHESTER, NEW YORK

The fuel cell power module for GM's Sequel was developed in Rochester, NY.

LEADING THE RACE TO BRING FUEL CELL TECHNOLOGY TO THE MASSES.

ROCHESTER, NEW YORK
Named one of the
TOP 20 TECH CITIES
in the country.
– *Popular Science*, March 2005

Did you know, much of today's fuel cell technology is driven by brain power generated in the Greater Rochester, NY Region? We have one of the nation's smartest workforces, including fuel-cell experts who research and manufacture "smart energy" solutions at General Motors and Delphi Fuel Cell Development Centers. We're also home to a clean energy business incubator and one of the nation's premier Hydrogen Technology Learning Centers at Rochester Institute of Technology. This skilled workforce, combined with world-class fuel cell research facilities and exceptional quality of life, puts Rochester, NY at the forefront of the industry. It also creates a rich supply of energy resources you can use to propel your business forward.

GRE
GREATER ROCHESTER ENTERPRISE

Discover the power to grow your business.
Visit **RochesterBiz.com/MIT** or call us toll-free at **877-805-1770.**

ENERGY

Hydrogen on the Cheap

This low-cost electrolyzer built by General Electric could help the hydrogen economy.

Wouldn't it be nice to have a machine that could cheaply manufacture a gallon of gas per hour for your automobile? Envisioning the day when we may all have fuel cell cars, General Electric researchers have built a prototype that makes the equivalent quantity of hydrogen: plug it in, and it splits water molecules to generate one kilogram per hour of hydrogen.

The basic technology, called an electrolyzer, is nothing new: water is mixed with an electrolyte and made to flow past a stack of electrodes. Electricity causes the water molecules to split into hydrogen and oxygen gases. What GE has achieved is a potentially inexpensive, mass-manufacturable version of the technology.

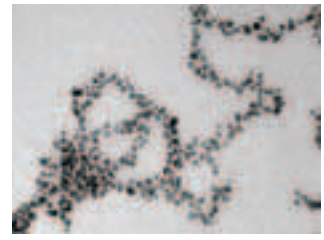
Whereas traditional electrolyzers are made with expensive metals requiring hand assembly, a team at GE Global Research in Niskayuna, NY, came up with a way to make them largely out of a GE plastic called Noryl that is easy to form and resistant to the highly alkaline potassium hydroxide electrolyte. To get more hydrogen out of a smaller electrode, the researchers borrowed a spray-coating process normally used for jet engine parts to coat the electrodes with a proprietary nickel-based catalyst that has a larger surface area.

Their prototype of an easy-to-manufacture apparatus could lead to a commercial version that produces hydrogen via electrolysis for about $3 per kilogram—a quantity roughly comparable to a gallon of gasoline—down from today's $8 per kilogram. "We've attacked the capital costs," says Richard Bourgeois, an electrolysis project leader. GE could potentially manufacture the machines within a few years, he says. **DAVID TALBOT**

NANOTECH

New Way to Sniff Drugs

Researchers in India say sniffing a special gold-particle solution could be a new way for diabetics to keep blood sugar under control. Physicist Murali Sastry and his colleagues at the National Chemical Laboratory in Pune, India, loaded insulin on the surface of gold nanoparticles about five nanometers in diameter by capping the particles with aspartic acid, an amino acid. The acid produces a charge that allows the insulin to adhere through electrostatic interactions. In results published this year, the technique reduced blood sugar levels in diabetic rats by up to 55 percent in about two hours, a drop comparable to the effect of standard insulin injections. The particles are rapidly absorbed



through the mucous membranes in the nasal tract; the Indian researchers say preliminary observations indicate the gold is expelled in urine. Since insulin-dependent diabetes is a chronic condition, clinical trials would have to wait until the group establishes that there is no bioaccumulation of gold. But if all goes well, the group says, the method could emerge as a new platform for delivering drugs that otherwise must be injected because they break down in the stomach. "We're looking at nanogold as a platform technology to deliver a range of drugs," says Varsha Pokharkar at the Poona College of Pharmacy. GANAPATI MUDUR

LONNY KALFUS (HYDROGEN); COURTESY OF VARSHA B. POKHARKAR (DRUGS)

Roomba

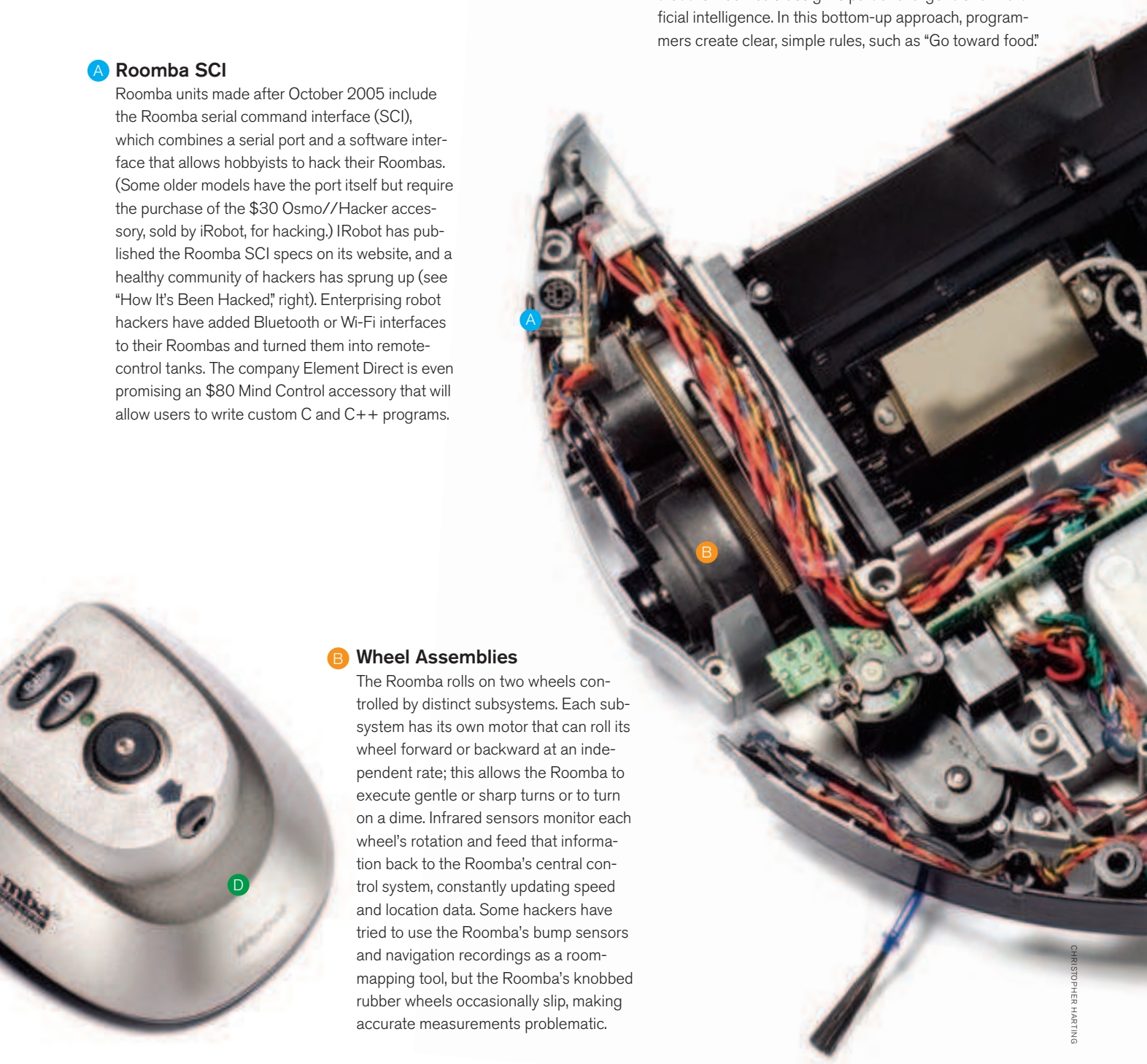
Two MIT grads and a professor took simple materials and rules and came up with the first autonomous robot to become a household phenomenon in the United States. By Daniel Turner

A Roomba SCI

Roomba units made after October 2005 include the Roomba serial command interface (SCI), which combines a serial port and a software interface that allows hobbyists to hack their Roombas. (Some older models have the port itself but require the purchase of the $30 Osmo//Hacker accessory, sold by iRobot, for hacking.) IRobot has published the Roomba SCI specs on its website, and a healthy community of hackers has sprung up (see "How It's Been Hacked," right). Enterprising robot hackers have added Bluetooth or Wi-Fi interfaces to their Roombas and turned them into remote-control tanks. The company Element Direct is even promising an $80 Mind Control accessory that will allow users to write custom C and C++ programs.

C The Brain

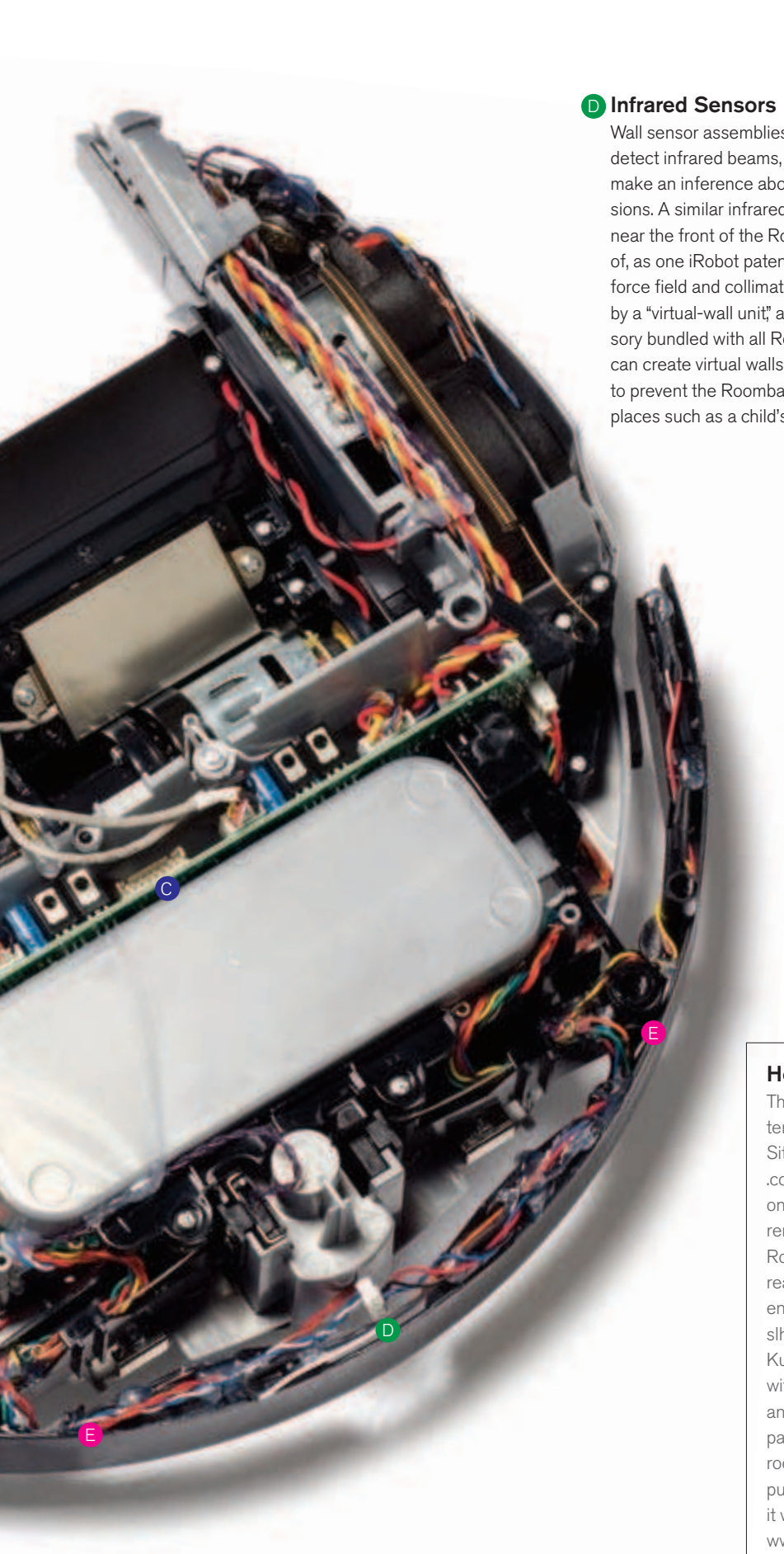
The Roomba is no supercomputer. In fact, its 16-bit Freescale Semiconductor microcontroller wouldn't cut it in a handheld game console. Still, this modest mind is strong enough to allow the Roomba to monitor itself 67 times per second and to follow a few simple but clever rules. IRobot is closemouthed about these algorithms, but turn on a Roomba, and it will spiral out, then move straight until it nears a wall, which it will follow until it finds another obstacle. Tod E. Kurt, cofounder of ThingM, a ubiquitous-computing research group, notes that the Roomba's design is part of a larger trend in artificial intelligence. In this bottom-up approach, programmers create clear, simple rules, such as "Go toward food."



CHRISTOPHER HARTING

B Wheel Assemblies

The Roomba rolls on two wheels controlled by distinct subsystems. Each subsystem has its own motor that can roll its wheel forward or backward at an independent rate; this allows the Roomba to execute gentle or sharp turns or to turn on a dime. Infrared sensors monitor each wheel's rotation and feed that information back to the Roomba's central control system, constantly updating speed and location data. Some hackers have tried to use the Roomba's bump sensors and navigation recordings as a room-mapping tool, but the Roomba's knobbed rubber wheels occasionally slip, making accurate measurements problematic.



D Infrared Sensors

Wall sensor assemblies send out and detect infrared beams, letting the Roomba make an inference about a room's dimensions. A similar infrared emitter/detector near the front of the Roomba takes note of, as one iRobot patent describes it, "a force field and collimated beam" sent out by a "virtual-wall unit," an external accessory bundled with all Roomba models. You can create virtual walls wherever you want, to prevent the Roomba from entering places such as a child's play area.

E Bump Sensors

Bump sensors are another simple mechanism that, coupled with simple rules, can produce what appears to be intelligent action. The spring-loaded bumper, when displaced by contact with an object such as a wall, a table leg, or a cat, interrupts a beam sent out by the infrared emitter/detector; this triggers a signal to the Roomba's control system, telling it to enter "bounce" mode. In this mode the Roomba turns in a best-guess direction and resumes its cleaning. The bumper also contains the Roomba's four "cliff detectors," which send infrared beams toward the floor. When there's a long delay in the beam's return, as when the Roomba starts to go over a stair step, the control system knows it's time to turn around.

How It's Been Hacked

The Roomba's low price and SCI port have made it a tempting entry-level platform for robotics experiments. Sites such as roombareview.com and roomba.pbwiki.com have sprung up, where enthusiasts can trade tips on hacks such as cobbling together Bluetooth or Wi-Fi remote controls out of spare parts. One Bluetooth-enabled Roomba was given a green fabric pelt and was used in a real-life Frogger game at the SXSW Interactive conference in Austin, TX, this year (www.secondlifeherald.com/slh/2006/03/realfrogger_tec.html), and ThingM's Tod E. Kurt is collaborating on a live-action Pac-Man re-creation, with reprogrammed Roombas dressed up as Pac-Man and ghosts, navigating a maze and vacuuming up tissue paper dots. RoombaNet (people.csail.mit.edu/bpadams/roomba), created as part of a PhD thesis, is a tiny computer that rides on the robot and can be used to control it wirelessly. And if you want to see a Roomba in action, www.vacuumcleanerlive.com has hooked a spycam to a Roomba for a first-person (first-robot?) streaming video.

Microsoft

GET THE FACTS.

TELEFLORA CHOSE WINDOWS SERVER OVER LINUX AND UNIX, AND SAVED 35% IN DEVELOPMENT COSTS.

"Developing our new POS system on Windows Server™ 2003 and .NET cost us 35% less than a Linux or UNIX solution, and we're able to deploy new features and new services twice as fast. That gives us and our 25,000 florist customers, a crucial advantage in our rapidly changing industry." –Jim Siplon, EVP/CTO

teleflora

For these and other third-party findings, go to microsoft.com/getthefacts

Windows Server™ 2003

George Church

Rewriting the genome

The genomic revolution is being driven by advances in analytical and computational techniques, and George Church has been behind many of them. Starting in the late 1970s, Church helped create the tools, including early software and protocols for DNA sequencing, that eventually made possible the Human Genome Project. These days, Church, a professor of genetics at the Harvard Medical School, and his 50-person lab are still finding ways to synthesize and sequence DNA faster and more cheaply. One of his latest interests is synthetic biology, in which researchers design and synthesize biological "parts" that they then incorporate into microbes or cells. Some anticipated products of synthetic biology: engineered cells that produce novel types of pharmaceuticals, redesigned biological therapeutics that are more effective and safer, and biosensors that can be built directly into cells.

***TR*: What is synthetic biology?**

Church: Genetics turned into genomics when you dealt with the whole genome. Biology turns into systems biology when you deal either with the whole of the cell or some fairly large part of it. Genetic engineering turns into synthetic biology when you use what you learn from parts and theory to engineer real systems.

How could synthetic biology help you design more-effective drugs?

Some groups are making cells that sense tumors and respond by producing a toxin. Synthetic biology will help you engineer the cell to home in on the tumor, to recognize the tumor, and, once it is confirmed, to start making a tumor-specific drug.

You and your colleagues recently developed a new way to synthesize DNA. What are the benefits?

It's about reducing cost at a reasonable accuracy. Right now the cost of synthesizing a base [using conventional technology] is about 10 cents. That's the current street price for raw oligonucleotides. For synthesizing simple genes, it's more like $1.30 a base. [Our method] can manufacture oligonucleotides at .01 cent per base.

How will getting the cost down aid synthetic biology?

It means you're willing to make many more [genetic] constructs. Making more constructs means you're much more likely to make something that works or something useful.

The new method also allows you to make longer stretches of DNA, right?

Longer stretches are certainly enabled. The implications are that we are getting closer to being able to arbitrarily "program" the millions of base pairs in microbes or billions of base pairs in plants and animal genomes similar to the way that we program computers.

There has been a lot of buzz about a $1,000 personal genome.

That's sequencing. So we're off synthesis now.

Right. Now we're talking about sequencing an individual's genome.

We might never get a perfect $1,000 diploid genome [the six billion base pairs in a human's two sets of chromosomes]. The question is, what can we afford and what do we get for it? Think back to the beginning of the computer industry. They didn't say, "Oh, we're going to get you a $1,000 supercomputer." No, they said, "What can people afford? And what can we give them for it?" And what they gave us was the likes of the Apple II computer, and people started writing software for it. Current personal computers cost about the same but deliver more. The same thing may happen with personal genomes.

So what are people likely to spend to know their own genome?

I think what is affordable—and remember, this is a lifetime expense; your personal genome will hopefully last you 80 years or more—is $10,000. If I can save $100 on average a year, it is a no-brainer. That's the cost of a couple days of missed work, or one diagnostic test that can be put off due to low risk, or avoiding bad choices on a year's worth of drugs. Then the question is, how much of a person's genome can we sequence for $10,000? Seven thousand dollars will buy you a million base pairs of DNA [using conventional technology], which is one-6,000th of your diploid genome. Not very much.

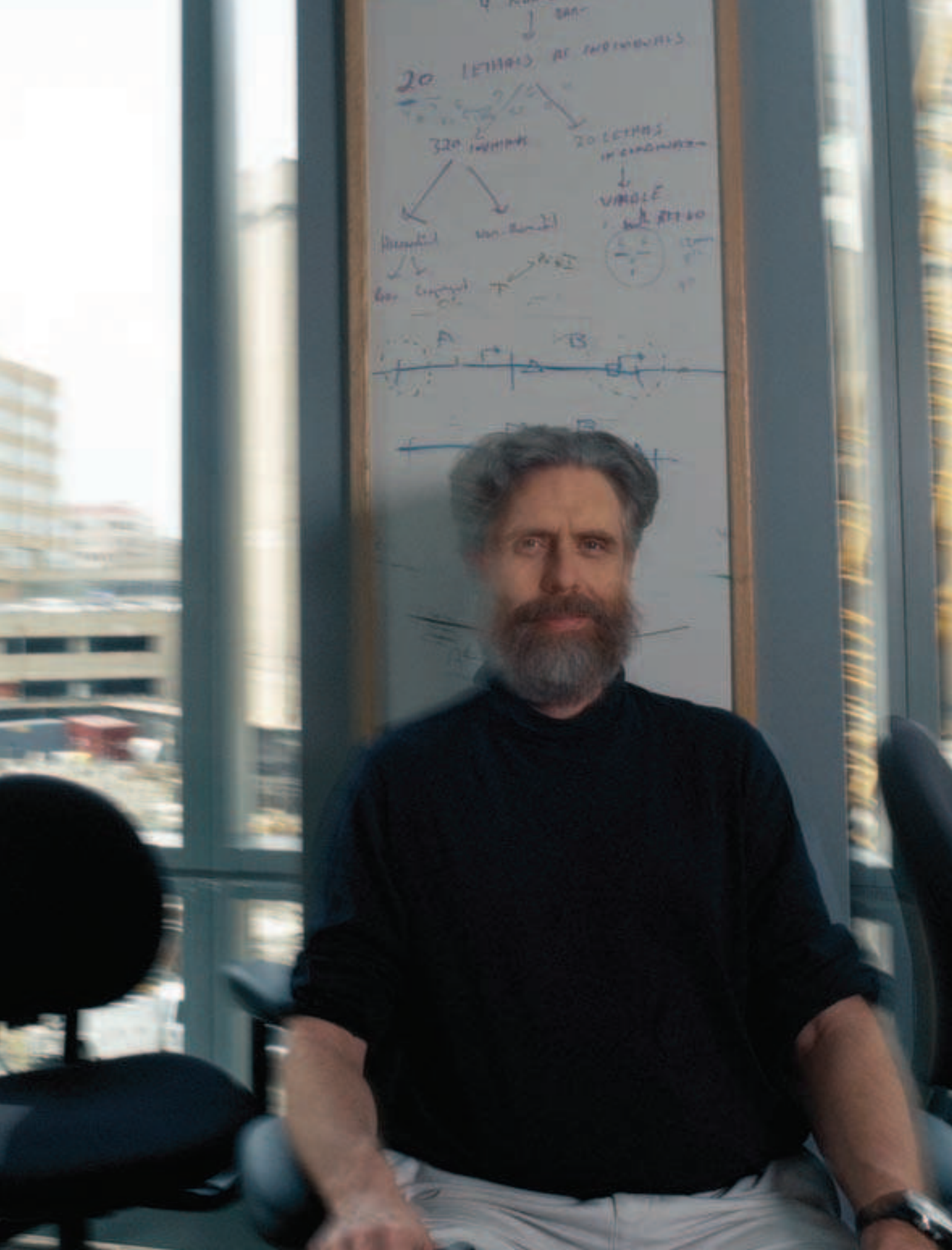
Polony sequencing [a method developed by Church and colleagues] is about a hundred times less expensive. So you can sequence about 1 percent of the genome [for $10,000]. That's not bad. You could focus on likely places you're going to have problems.We got a factor-of-ten improvement in the last six months, so if we could get another 10 percent improvement in the next year, that would give us 10 percent of the genome. If we could pick 10 percent of the genome for which we have lifestyle, nutritional, or synthetic solutions, that would be a good deliverable for a $10,000 investment. And it will just get better from there.

We jumped from synthesis to sequencing.

I do that all the time. It may sound like a wordplay, but it is actually a very fundamental concept. There is almost no synthesis that doesn't involve sequencing, and vice versa. And that is why I have really emphasized this connection in my lab. They are very synergistic.

DAVID ROTMAN

MARK OSTOW



BIOTECHNOLOGY

Stem Cell Hope

Cellular reprogramming, argues **Robert Lanza**, could make moot the ethical debate surrounding stem cells.

Embryonic stem (ES) cell research, we hope, will be moving from the laboratory to the clinic in the coming years. The promise of this technology—and the associated scientific challenge—is enormous *(see "Stem Cells Reborn," p. 58)*. Worldwide, 17 million people die every year from cardiovascular disease, more than 200 million suffer from diabetes, and millions more fall ill from a wide range of other disorders that may one day be treatable with stem cell therapies. It's possible that, in addition to generating an unlimited supply of functional replacement cells, ES cell progeny could be used to reconstitute more complex tissues, including blood vessels, bone, and even entire organs such as kidneys or hearts. But even if stem cell researchers learn to generate these various tissues, doctors still will not be able to transplant them into patients without either the risk of immune rejection or the use of immunosuppressive drugs that can lead to a wide variety of serious and potentially life-threatening complications.

Somatic-cell nuclear transfer (SCNT)—also known as therapeutic cloning—could potentially prevent the immune responses associated with the transplantation of ES cell–derived tissues. Unfortunately, however, using SCNT to treat everyone with cardiovascular disease and diabetes alone would require several billion (yes billion!) human eggs, and at present, it is proving problematic for researchers to obtain even a limited supply of human eggs for research purposes. Of course, aside from the problem of egg supply, there's also the debate over the ethics of creating—and destroying—hundreds of millions of human embryos to generate patient-specific stem cell lines.

Fortunately, there's a new area of stem cell research that aims to bypass the need for human eggs and even the creation of embryos. Scientists hope to reprogram patients' cells in the laboratory so that they enter a stem cell–like state where they have the potential to turn into some (multipotential) or all (pluripotential) of the 200-plus cell types in the body. Such advances will hopefully allow us to produce youthful cells and tissues that are genetically compatible with patients. These cellular-reprogramming technologies could become the treatment of choice for chronic diseases. In the same way that the ooplasm of an egg is capable of reverting the nucleus of any cell back to an embryonic state, the cytoplasm of other cell types (such as blood cells) may be capable of reprogramming another cell type (such as a skin cell). This technology has the potential to transform mature body cells extracted from a patient into pluripotent stem cells, while sidestepping the ethical debate associated with both egg cells and embryos.

Unfortunately, it's unclear whether this goal can be achieved in a few years, or whether it will take decades. To begin with, more research is needed to explain how the egg ooplasm is able to take a fully differentiated nucleus backward in time and turn it into a totipotent cell that has the capacity to generate an entire organism. There is also tantalizing evidence that ES cells can be used instead of eggs to reprogram somatic cells. Does the magic lie in the cytoplasm or the ES cell nucleus? While you are reading this, dozens of groups worldwide are actively trying to answer this and other questions associated with cellular reprogramming. With a little luck, one of them might get stem cell research out of its ethical bind. TR

Robert Lanza is vice president of medical and scientific development at Advanced Cell Technology.

INFORMATION TECHNOLOGY

On the Grid

Grid computing is becoming an affordable utility for everyone, says **Jonathan Schwartz**.

A few years ago, I had a series of meetings with CIOs and CTOs in New York City. I asked them all the same question: "Do you feel the grid you're building is delivering a competitive advantage to your business?" (When we talk about a computer grid, we ordinarily mean a private collection of low-cost network, storage, computing, and software elements, lashed together to do complicated computing work that historically required multimillion-dollar data centers.)

I asked the same question of researchers and executives in the energy industry, which is using grids to find oil; the life sciences, where grids help in drug discovery; the motion picture industry, where grids are used to render complex effects and animation; and academia, where grids are supporting all sorts of innovative science.

The answer was always the same: "Absolutely, yes. Our grid is way better than any of our competitors'." The only problem: computing is evolving in a completely different direction.

As strange as it may sound, consumers are way ahead of most enterprises and academic institutions when it comes to using *public* grids (and

ILLUSTRATIONS BY MARC ROSENTHAL

paying for them). Most of us now live on the public grid at home. We don't need a supercomputer in the garage; we use the Internet to access Google and Yahoo, we love eBay, we bank from home, we upload and share photos on Flickr and movies on YouTube, and we gather our news from various sources across the Web.

Yet most major research institutions and corporations are still reluctant to leverage "utility computing"—computing power provided on demand over the open Internet. To me, that's like living without electricity.

But there are signs that change is afoot. A good friend of mine, a bioinformatician, described how frustrated he was at having to wait while his university's private supercomputing facility worked through its queue of pending jobs to get to his. "If you had a grid available online, I'd bring my whole budget to you," he said. Granted, his budget was only about $10,000 per quarter, but I assure you there's a good business in serving the "long tail"—the multitude of users with narrow interests and needs that, in aggregate, are the majority.

I believe that in the not-so-distant future, most computing power available over the Internet will be purchased by that tail. There are, after all, far more small businesses than large ones. I'm very comfortable betting on the value in volume—and the willingness of those smaller firms to change culture, process, and lifestyle to get a competitive advantage through network services.

The simplicity, accessibility, and affordability of a true Internet utility computing service will change the face of computing for all organizations, large and small, public and private. And they won't have to house the grid, manage it, power it, provision it...or buy it. TR

Jonathan Schwartz was named chief executive officer of Sun Microsystems in April.

NANOTECHNOLOGY

Nitrogen Fix

Richard Schrock describes why finding an elusive catalyst could have a surprising impact on energy consumption.

Molecular nitrogen (dinitrogen, N≡N) makes up about 78 percent of the atmosphere. It is the most unreactive diatomic species known. Interestingly, however, nitrogen is required for all life; it is used to build proteins and DNA. Therefore, dinitrogen must be turned into a molecule that can be assimilated readily by plants. That molecule is ammonia, NH_3.

Prior to World War I, the iron-catalyzed Haber-Bosch process for ammonia synthesis at high temperatures (350 to 550 °C) and pressures (150 to 350 atmospheres) from dinitrogen and dihydrogen (H_2) was discovered. It is perhaps the most important industrial process ever developed and responsible for a dramatic increase in the population of the earth during the 20th century, because it supplies a reliable source of nitrogen for fertilizers. But because the Haber-Bosch process requires high temperatures and pressures, it consumes tremendous amounts of energy; it is estimated that as much as 1 percent of the world's total energy consumption is devoted to the process.

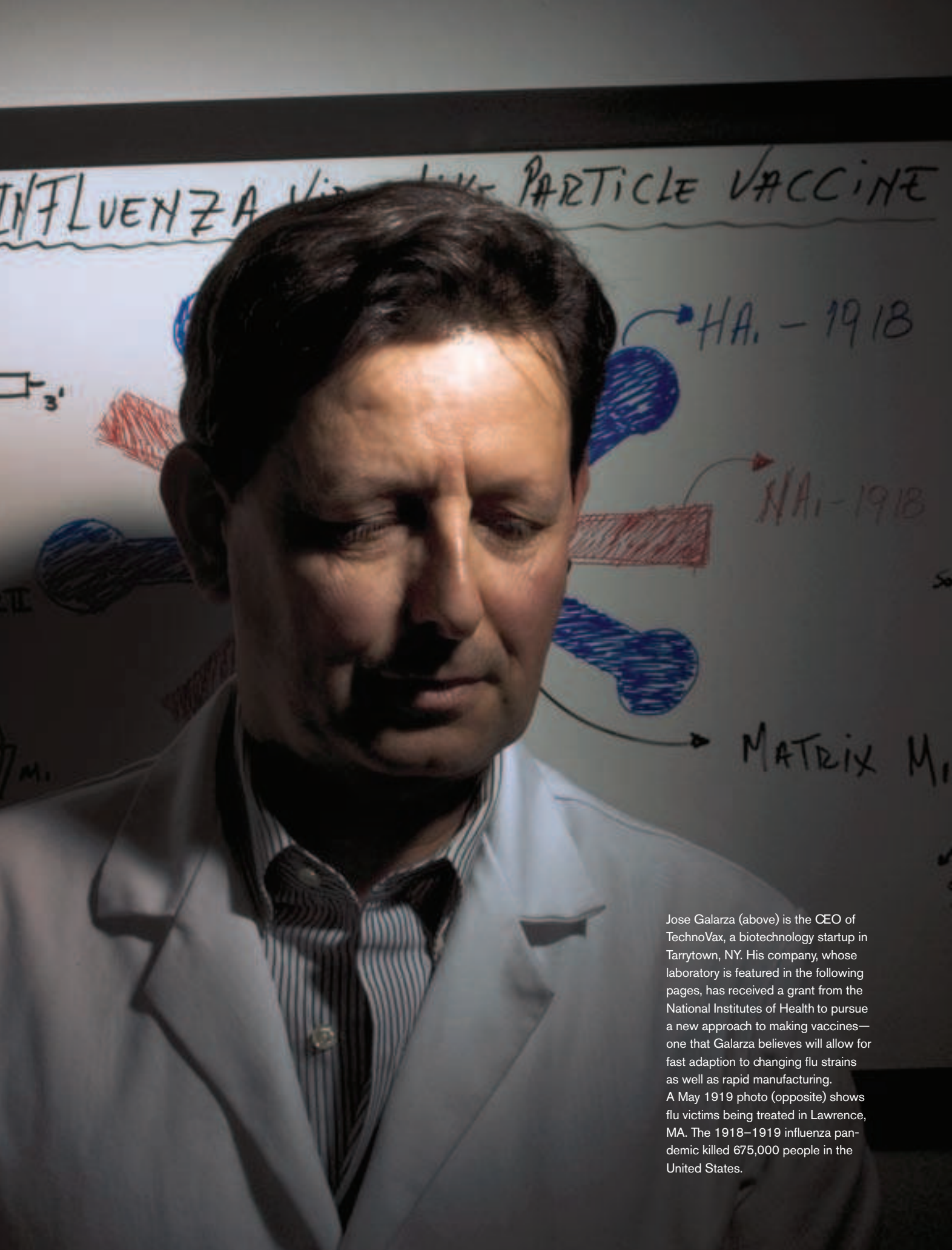
Nature also reduces dinitrogen using metalloenzymes in bacteria and blue-green algae, but at only one atmosphere of pressure and mild temperatures. The metalloenzymes, called nitrogenases, contain iron and usually molybdenum. Ever since their discovery more than 40 years ago, chemists have speculated about how reduction of dinitrogen occurs and whether an "artificial" nitrogenase could be developed that would lead to a more energy-efficient process than Haber-Bosch. Perhaps a thousand man-years and billions of dollars have been spent studying how nitrogenases work and trying to make artificial ones.

In 2003, my group showed that it is possible to make ammonia catalytically from dinitrogen, protons, and electrons. This is accomplished at a *single* molybdenum metal center. In the presence of protons and electrons in a nonaqueous medium, dinitrogen is reduced to ammonia with an efficiency in electrons of around 65 percent; the remaining electrons are used to make dihydrogen, which is in this context a wasteful and undesirable product. Our catalyst is not great, but it is a start.

Nature has developed a highly optimized version of the nitrogen reduction process over a period of a few billion years. Ours is an "artificial" nitrogenase that is barely catalytic. We are trying to identify the key problem or problems that prevent it from working well. Perhaps then we can improve its efficiency.

Can we design catalysts that will be as efficient as natural nitrogenases? Possibly. Will the Haber-Bosch process ever be replaced by catalysts that do not operate at high pressures and temperatures? Unknown. Only time, money, and ingenuity will reveal the answer. TR

Richard R. Schrock, the Frederick G. Keyes Professor of Chemistry at MIT, won the 2005 Nobel Prize in chemistry.



Jose Galarza (above) is the CEO of TechnoVax, a biotechnology startup in Tarrytown, NY. His company, whose laboratory is featured in the following pages, has received a grant from the National Institutes of Health to pursue a new approach to making vaccines—one that Galarza believes will allow for fast adaption to changing flu strains as well as rapid manufacturing.
A May 1919 photo (opposite) shows flu victims being treated in Lawrence, MA. The 1918–1919 influenza pandemic killed 675,000 people in the United States.

Photo Essay

Catching the Flu

In 1918 and 1919, the Spanish flu killed an estimated 50 million people worldwide. Today, health experts worry that if the virulent avian flu were to mutate into a strain that humans could easily contract and spread, the world could face a similarly devastating pandemic. In an effort to develop new flu vaccines more quickly and at lower cost, researchers funded by major bodies like the National Institutes of Health and the U.S. Centers for Disease Control and Prevention are working on vaccines for the 1918 flu virus itself. They hope to learn what made it so contagious and deadly.

By Stephan Herrera Photographs by Sean Kennedy Santos

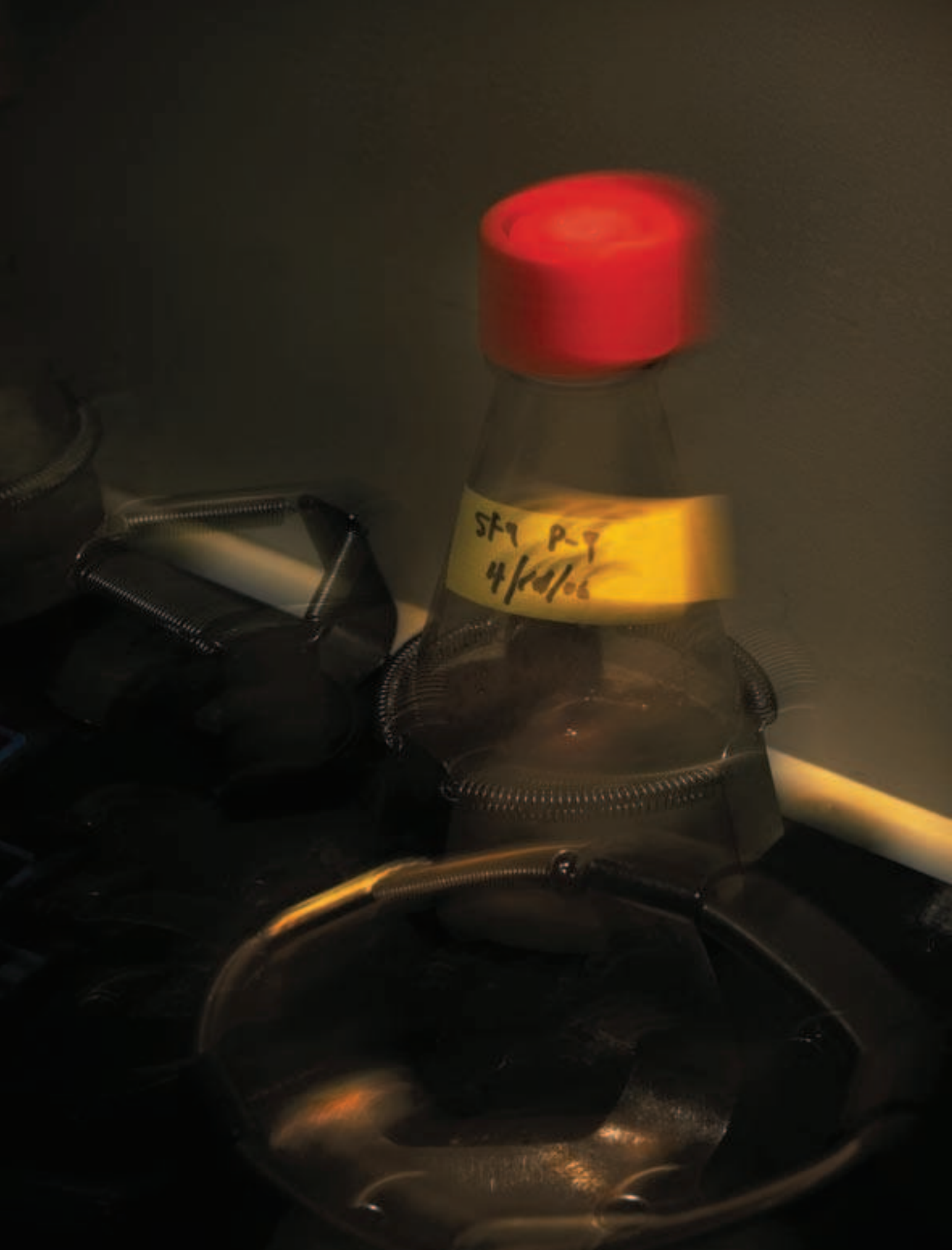
BETTMANN/CORBIS

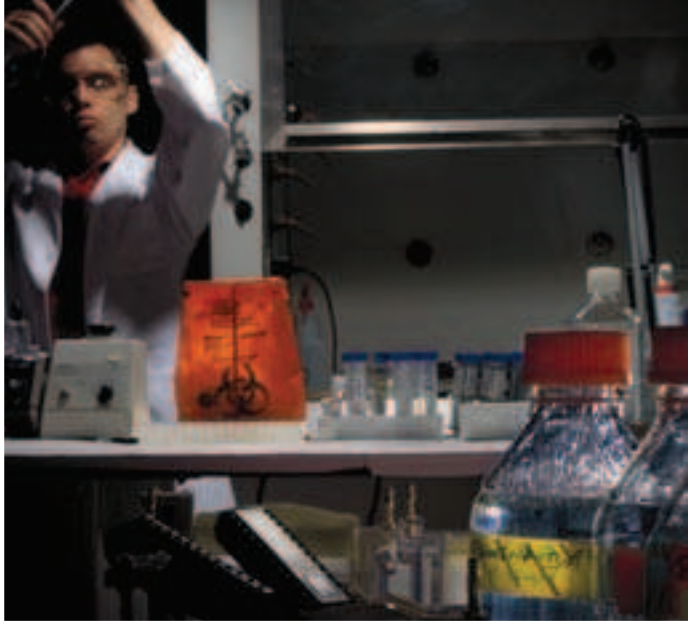
The 1918 virus (above) can be a useful test target for vaccines made by novel methods. Jose Galarza, whose NIH grant has him using just a portion of the virus, works with viruslike particles (VLPs), balls of protein arranged to so closely resemble a virus that they provoke an immune response. VLPs can thus serve as the basis for a vaccine, but because they do not contain a virus's genetic material, they can't replicate and cause infection. When freeze-dried, they can also last for six weeks, which makes them easy to transport.

Galarza says that his company's VLPs self-assemble quickly enough to be made in large quantities in weeks. Vaccines made the traditional way—grown in chicken eggs—require months to produce.

Galarza makes his VLPs with the aid of insect cells, which, in a process called transfection, have foreign DNA inserted into them. The extra DNA directs the synthesis of the VLP proteins and controls their release to the cells' surfaces. A shaker incubator (right) agitates a flask to oxygenate the insect cells inside it and keep them in suspension.

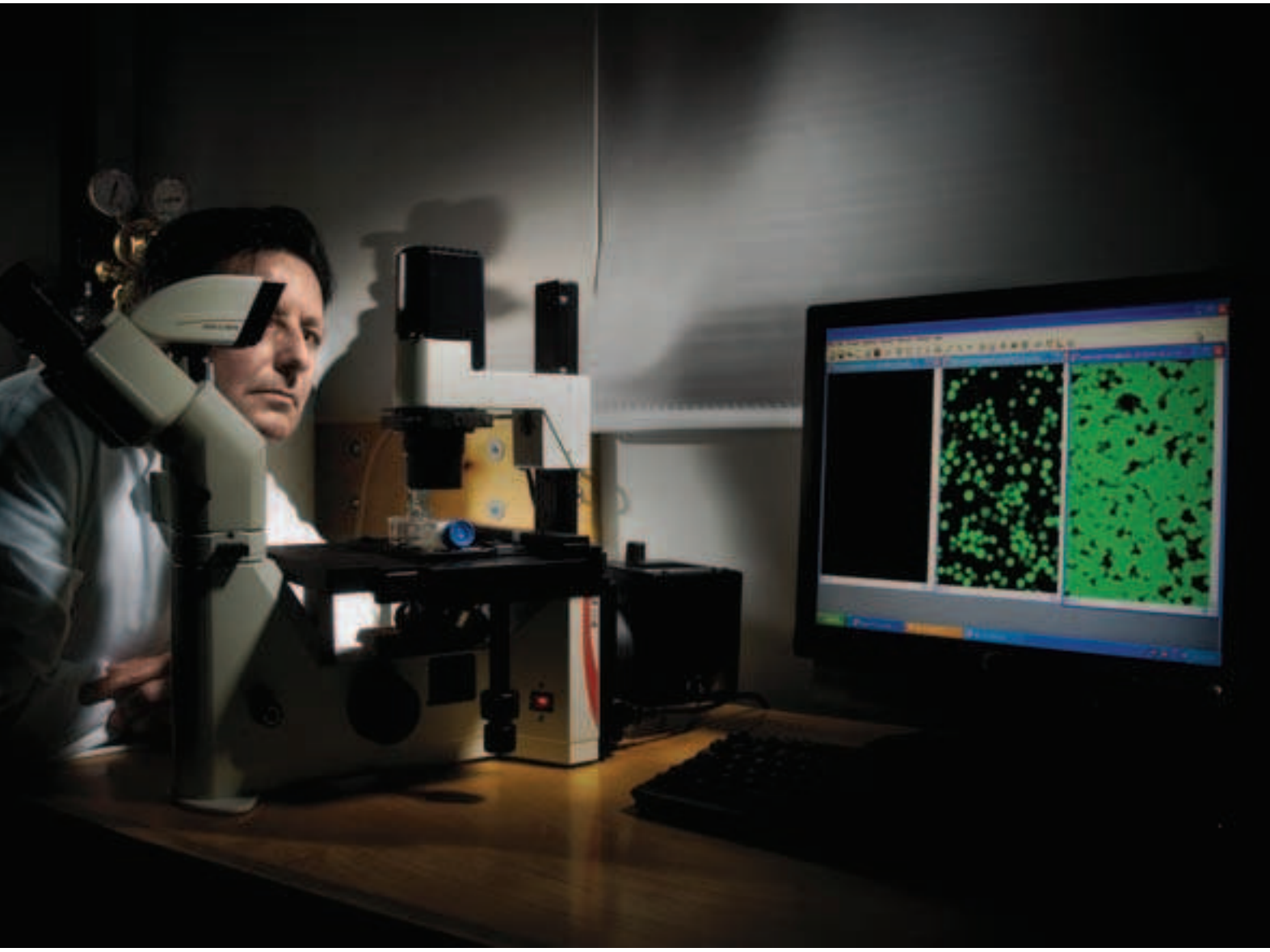
COURTESY OF CDC/ TERRENCE TUMPEY





The development of a new VLP vaccine begins with the extraction and purification of the genes that code for the VLP proteins. At the end of the extraction process, purified DNA precipitates out of solution in a flask; along the way, the solution changes color to indicate the conclusion of each stage in the process. The purified DNA is placed in a polymerase chain reaction machine (above, bottom) to be copied.

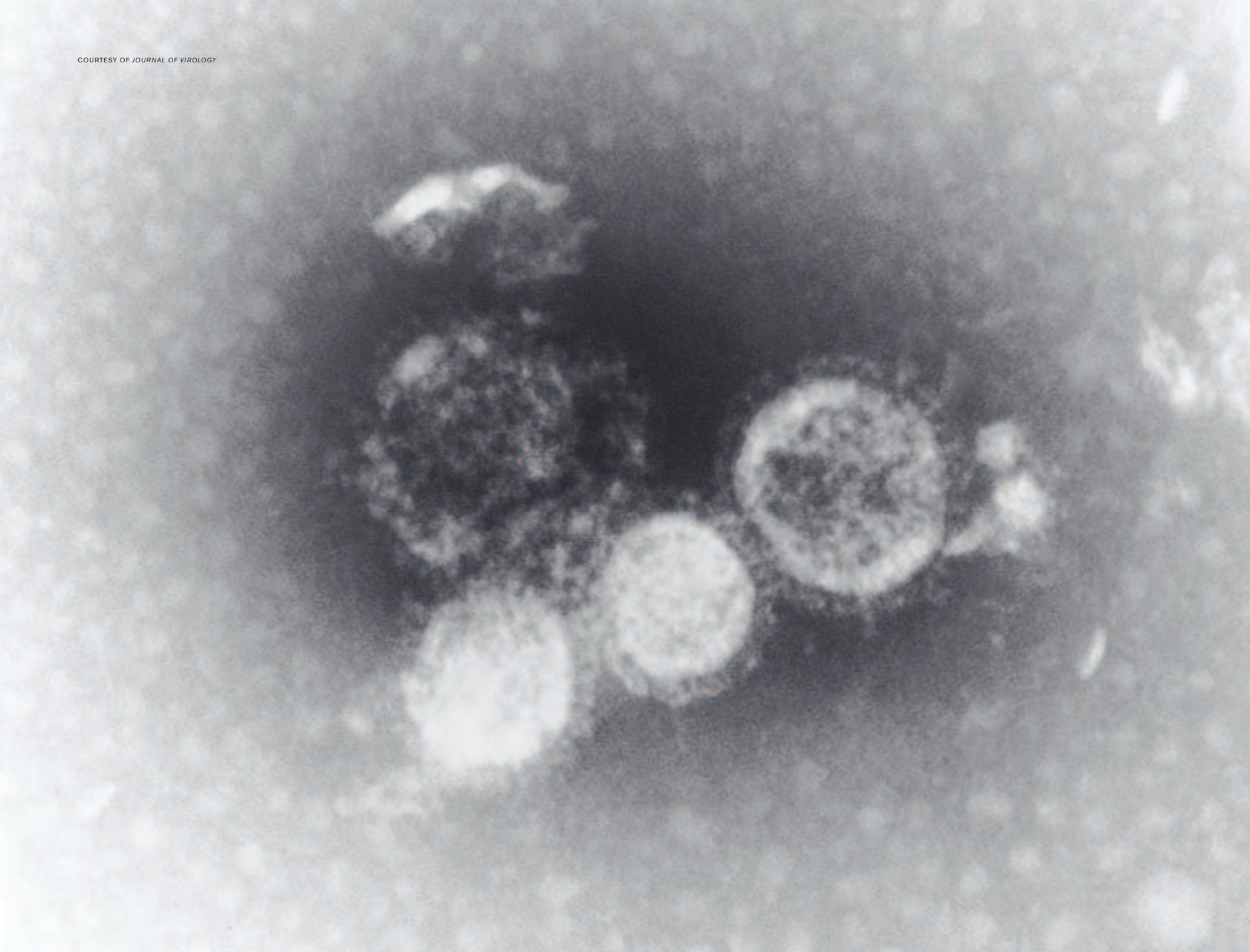
Researchers then string together the genes for the various proteins that will make up the VLP (above, top). Once those genes have been introduced into the insect cells, the cells are microscopically examined to determine whether they are producing the desired proteins. All work with the cells takes place in a biosafety cabinet workstation (left).



Current efforts to make flu vaccines face a central difficulty: the lag time between when a new flu strain is identified and when a vaccine against it can be produced is long enough to allow for a pandemic. Currently, the H5N1 avian influenza is what most concerns health officials (the deadly 1918 virus was also an avian flu). But unless the lag time for vaccine development shortens, there are certain to be similar worries in the future.

If VLPs can yield vaccines quickly and cheaply, they could allay some of those worries. While their efficacy has yet to be proven, it is clear that VLPs can be produced in great quantities, quickly. In the photo above, the images on the monitor depict the number of VLPs produced by a culture of cells on three consecutive days. The green glow indicates that the VLP production is progressing as planned. The photo on the opposite page was taken in 2001; it shows VLPs that Galarza produced while working for Wyeth, a Madison, NJ–based pharmaceutical company.

Galarza's NIH grant funds his work on vaccines for four different strains of flu: the 1918 flu; the H5N1 avian influenza that is spreading across Asia and Europe; the H7N7 avian influenza, which hit the Netherlands in 2003; and the current seasonal New York strain of influenza.



COURTESY OF *JOURNAL OF VIROLOGY*


CONTENT ENHANCED & PROTECTED

By Wade Roush

Inside the Spyware Scandal

Last year, Sony BMG put antipiracy software on their CDs. In so doing, they spied on their own customers and gave hackers the power to access people's computers. What were they thinking?

John Guarino is the owner of TecAngels, a two-man computer consultancy in Manhattan. Give Guarino your ailing Windows PC, and in two or three hours he'll return it to you in perfect health. Often, he can solve his customers' problems over the phone.

But last summer, Guarino came across a problem he couldn't fix. In the process of flushing out the spyware and viruses infecting his customers' computers, he began to find the same mysterious intruders in machine after machine. They were strangely named files lurking deep inside the "registry" where Windows stores settings and instructions that control all of a computer's hardware and software.

To Guarino, the files looked like a rootkit—software that tricks an operating system into overlooking worms, viruses, and any other files a hacker might want to conceal inside a user's computer. The files didn't seem to be causing damage, and Guarino's antivirus software didn't identify them as threats. But they had appeared on people's hard drives uninvited—the conventional definition of "malware"—so Guarino removed them.

But the files didn't go quietly. After Guarino deleted them, the CD drives on his customers' computers would stop working. The usual solution—reinstalling the software that drives the disc players—didn't correct the problem. Guarino couldn't explain this odd effect, and his customers weren't paying him to spend hours researching it; they just wanted their computers back. So he would usually resort to the nuclear option: reinstall the operating system from scratch.

After six or seven of these encounters, Guarino was growing weary. Then, on September 30, he discovered the mysterious files on his own PC. "That's what really pissed me off," Guarino says. "I was like, 'I can't believe it. I have the latest firewall, the latest antivirus software, three or four antispyware programs. How did this get here?'"

Like any good investigator, Guarino backtracked. He knew that the files hadn't been there the last time he had scanned his computer. He tried to reconstruct everything he had done with his machine over the previous few days—what programs he had installed, what e-mails he had received, what websites he had visited.

Then he remembered that he had purchased a music CD the day before and had played it on the computer. It was a Sony BMG Music Entertainment album called *Touch*, by the rhythm-and-blues singer Amerie. Unlike most CDs, this disc couldn't be played using common media-player software such as iTunes, RealPlayer, or Windows Media Player. To hear the CD, purchasers had to install the customized Sony BMG player included on the disc. Guarino had done this.

Now he took a closer look at the CD's jewel box. One phrase popped out at him: "Content Enhanced and Protected." Evidently, the disc carried some form of digital rights management (DRM) software—a program designed to control copying and thus discourage piracy.

Finally, the pieces came together. The mystery files resembled a rootkit; the usual purpose of a rootkit is to hide something; a copy protection program was the kind of thing its

MATT CARR

creators might wish to hide from users; and removing this particular rootkit disabled the CD drive. Guarino could only conclude that the malware's source was Sony BMG itself.

"That's when I gave up," Guarino says. He could fight malware one machine at a time. But if the world's second-largest record company wanted to install secret software on its customers' computers, he would never win.

Before putting the problem aside, Guarino did one very important thing. He e-mailed his logs to F-Secure, a computer security firm in Helsinki, Finland, whose software he had used to detect the files. Though F-Secure's malware watchers had not previously encountered the rootkit, they were quickly able to confirm Guarino's suspicions. Over the next two weeks, they came to another, much more troubling realization: the rootkit could hide other files as easily as it hid Sony BMG's copy protection software. Every computer that had ever been used to play a copy-protected Sony BMG disc was now, in effect, an open receptacle for worms, viruses, and other malware.

On October 17, F-Secure contacted Sony. Two weeks later, respected security expert Mark Russinovich found the rootkit on his own computer and publicized his findings on his widely read blog. He also discovered that other software installed along with the copy protection program secretly contacted Sony BMG via the Internet every time a PC user played a copy-protected disc. And over the next several months, what had begun as a curiosity in Guarino's little shop escalated into a full-blown scandal, complete with backroom negotiations, public exposés, heated denials, angry boycotts, vengeful lawsuits, and rueful apologies.

Though its original purpose was to hide software that prevented listeners from making more than three copies of their music, Sony BMG's rootkit became the most public symbol to date of the perceived excesses of DRM technology—and of the growing suspicion media companies seem to harbor toward their own customers. The scandal is still having repercussions. It has reignited a dispute in the public sphere over the ways consumers should be allowed to use copyrighted digital information and, conversely, just how far copyright holders can go to secure their intellectual property against piracy. *(See "Who Will Own Ideas?", a* TR *special package published in June 2005.)*

Taken to extremes, experts say, digital rights management not only curtails people's right to make "fair use" of copyrighted material, which is guaranteed by U.S. copyright law, but can even create new technological hazards. "When you build computer systems where you're not protecting the user, but something from the user, you have very bad security," says Bruce Schneier, a luminary in the field of computer security and chief technical officer of Counterpane Internet Security in Mountain View, CA. "That's my biggest fear—this notion that the user is the enemy."

The story of the Sony BMG rootkit fiasco is about more than bad corporate judgment or the ongoing struggle over the rights of consumers to do what they want with the things they own. It is also about fear and the excesses it can arouse. When media companies apply such powerful, secret tools to content protection, it suggests that their nervousness over piracy has turned to panic. Although Sony BMG insists that the rootkit was deployed unintentionally, the episode persuaded many observers that the music industry had come to see deception as an indispensable component of digital rights management. It should be no surprise when customers who feel they are being treated like thieves stop buying things. If there is one message in Sony BMG's experience for other companies entering the digital world, it is that distrust engenders distrust.

Schoolyard Piracy

Demand for digital "content" (a feeble but convenient jargon word for everything from poetry to podcasts) is greater than ever. Sales of downloadable music worldwide nearly tripled between 2004 and 2005, from $380 million to $1.1 billion, and now represent about 6 percent of all music sales. As of March 2004, Apple's iTunes music store was selling songs at a pace of about 2.5 million per week. According to the U.K. version of *Macworld* magazine, it now sells three million songs every day.

Sony BMG's rootkit became the most public symbol to date of the perceived excesses of digital rights management—and the growing suspicion media companies seem to harbor toward their own customers.

One might expect content producers and distributors to be thrilled by digital's takeoff. But in reality, they are often preoccupied with the ever present threat of rampant copying. And for good reason: in a one-month period in 2005, 3.8 million U.S. households downloaded music using the free peer-to-peer file-sharing services WinMX and Limewire, while only 1.7 million households purchased files from iTunes, according to market research firm NPD Group. The Recording Industry Association of America puts the lost retail revenues from digital music piracy at $4.2 billion per year, and it has fought illegal downloads aggressively: in February, it announced that it had launched 750 new lawsuits against users of peer-to-peer file-sharing networks, bringing the total since 2003 to more than 18,000.

Preceding almost every illegal download, however, is a much more innocent act: ripping compressed computer files, such as MP3s, from a legitimately purchased CD. Ripping and burning CDs for personal use is perfectly legal in the United States. But Thomas Hesse, president of global digital business for Sony BMG, says it accounts for two-thirds of all piracy. "The casual piracy, the schoolyard piracy, is a huge issue for us," he told the Reuters news service last year.

So recording companies like Sony BMG are naturally attracted to technologies that promise to thwart wayward fans. Enter digital rights management, an industry that emerged in the late 1990s to help publishers and studios maintain control over the contents of DVDs, software, and the like. For DRM companies and their clients, "control" means barring customers from opening digital files unless they have paid to do so. It means preventing the copying, printing, backing up, or replication of a work except when expressly permitted by the work's license agreement.

For years the recording industry didn't need this level of control, since consumer-grade CD players (introduced in 1982 by Philips and Sony) were designed exclusively to play music, not to export it in digital form. But by 1996, when PC manufacturers began to include CD-ROM drives as a standard feature in home computers, the threat of "casual piracy" had emerged; and when it debuted in 1999, Napster, the first popular Internet music-sharing system, made good on that threat. Recording companies began to lobby in Washington for greater legal penalties against those caught sharing files—and also began looking for ways to make copying and sharing more daunting for the average user.

This isn't a straightforward matter. Protected discs must include DRM software to limit copying; yet at the same time, they must be playable on ordinary CD players. One way to meet both needs is to make CDs more like CD-ROMs, which often contain multiple "sessions" similar to the cuts on old vinyl LPs. The first session of a multisession CD, starting at the center of the disc, contains music, and the outer sessions contain software. Normal CD players read only the first session and ignore the rest, while a Windows PC with its "autorun" feature turned on looks first for programs in the outer sessions that it can execute. (Luckily for DRM developers, autorun is activated by default in Windows XP, and most users never change this setting.)

When Sony BMG undertook the industry's first large rollout of copy-protected CDs in 2005, it used the multisession method. On 52 Sony BMG albums released between January and November, the outer sessions included a Windows copy protection program called XCP (eXtended Copy Protection), which Sony licensed from a U.K. company called First 4 Internet, and a dual Macintosh/Windows program called MediaMax, from Phoenix, AZ–based SunnComm. This wasn't the first time a label had attempted to sell CDs with anticopying software; Arista Records, a Sony BMG subsidiary, marketed a disc carrying MediaMax in late 2003, and rival Macrovision's DRM software appeared on thousands of CDs from other labels beginning in 2002. What *was* unusual about the new Sony BMG discs, however, was the technique First 4 Internet had chosen to make XCP invisible.

Cloaking Device

When Sony originally hired First 4 Internet, it wasn't to build a DRM system for consumer CDs. According to press interviews with First 4 Internet executives months before the rootkit scandal broke, it was to deter copying of prerelease music by the label's own employees and contractors, and other recipients. The company's first DRM product, XCP1, rendered the music session on multisession CD-Rs, the type of recordable CD used in music studios, unplayable by computers. That ability was attractive not just to Sony BMG but also to its three major rivals, Universal, EMI, and Warner Music Group, all of which had licensed XCP1 by 2002.

But this method wouldn't work for consumer CDs, which needed to be playable in all types of devices, including computers, DVD players, video CD players, and ordinary players. So First 4 Internet developed a new program, XCP2, that uses a cleverer, slightly more permissive approach called "sterile burning." This unappetizing term simply means that purchasers of a protected CD can rip it to their computers, then burn copies back to blank CD-Rs, but those copies cannot be used to make more copies. (XCP2 came to be known simply as XCP.)

According to Princeton University computer scientists Ed Felten and J. Alex Halderman, who "reverse-engineered" XCP as part of an academic investigation, the software has several distinct functions that are invoked separately. The first time an XCP-protected disc is loaded into a computer, it asks the user to consent to Sony BMG's end-user license agreement (EULA). It then copies a number of programs and drivers to the hard drive and launches a proprietary media-player program. Once installed, according to a white paper Halderman and Felten published in February, the new drivers listen for attempts by other media players such as iTunes to read audio tracks on the CD; if they detect one, they replace the data returned by the CD drive with random noise. Meanwhile, a "back door" in XCP allows the proprietary media player to read the disc's raw data without distortion.

Built into the media player is a burning application that allows the owner of the CD to rip up to three copies of it and burn them to CD-Rs. These copies will contain everything on the original disc, including the audio tracks, the media player, and the copy protection software. But they will be sterile: the burning application will be disabled, meaning the copies can only be played, not ripped and burned again. Alternatively, users can rip individual tracks or entire

albums to their hard drives, then burn up to three copies to CD-Rs in the Windows Media Audio format.

If it were easy for users to sidestep or disable all of these complex functions, the copy protection system would be useless. And here is the nub of the controversy over XCP and the Sony BMG discs: First 4 Internet's developers decided that a number of the program's files and operations should be hidden from average users. The drivers that interfere with other media players' attempts to read a protected CD, for example, needed to be stored in a secret place where users couldn't find and remove them. Then there was the file XCP uses to count the number of copies of the CD the user is still permitted to make. The burning application is disabled only when the counter reaches zero. If advanced users were able to find this file, they could potentially change the counter's value back to three after each copy they burned.

Secrecy itself is routine in the software industry, but this was different. First 4 Internet achieved secrecy using a rootkit, then Sony BMG neglected to tell its customers about the program's presence or to provide a straightforward way to uninstall it. The term "rootkit" derives from computer networks using Unix-style operating systems, where the system administrator—the person with all rights and privileges to change the system—is said to have "root" access. The first "root kits," written in the mid-1990s, were collections of software tools used by Unix hackers to acquire root access and deposit rogue code without leaving a trail. Windows rootkits emerged in 1999 and became so commonplace that they could be downloaded free from hacker collectives such as the one that produces the online magazine *Rootkit* (www.rootkit.com). More sophisticated versions could be purchased on the Internet for a few hundred dollars.

First 4 Internet executives, citing ongoing legal action, would not answer *Technology Review*'s questions. Therefore, we do not know whether or not the company's developers knew that they were creating a rootkit, or whether they modeled XCP upon one of the open-source or commercial rootkits. However, outsiders who examined XCP's code found that it contained some open-source components, including code from one program that encodes music in the MP3 format and another that encrypts and decrypts music downloaded from Apple's iTunes. (The latter was apparently part of a never implemented plan to make XCP compatible with iTunes, according to Halderman.)

Another unknown is whether XCP's developers were aware that a rootkit, once installed on a customer's computer, could open a passage for other viruses and Trojan horse programs. But Princeton's Halderman says programmers at First 4 Internet must have been aware that the cloaking method they were employing was well known to malware writers. "They had to learn about this technique from other sources," Halderman says. "And in the course of researching how to use this technique, it's almost inconceivable that they wouldn't have discovered that [cloaking other malware] is something that rootkits do."

In any case, the company's hiding technique was highly effective—so much so that no security expert noticed the rootkit for at least six months after the release of the first copy-protected discs. But soon after Russinovich posted his report, malware authors discovered that they could use the rootkit to keep anything from viruses to spyware out of the operating system's view. Indeed, less than two weeks after the Sony BMG rootkit came to light, the first malware program designed to exploit it had surfaced. It was a "backdoor Trojan" called Troj/Stinx-E designed to hide itself inside the rootkit and allow other programs to take over users' computers via connections to an instant-messaging system called Internet Relay Chat.

The Finnish Connection

F-Secure is headquartered in a boxy glass-and-aluminum building on Helsinki's outskirts, just a block from the factory where Nokia—long before it became a cell-phone company—made thousands of kilometers of steel cable as part of Finland's massive war reparations to the Soviet Union.

Dominating F-Secure's second-floor command center are three big video screens. One depicts the architecture of a well-known computer virus as if it were a giant, spinning space station. Another shows a real-time map of malware activity worldwide. Mika Stahlberg, a research manager at F-Secure, is using the third screen to illustrate XCP's stealth features.

"I can demonstrate using the Van Zant album," Stahlberg says. He inserts *Get Right with the Man*, a country album by veteran rockers Johnny and Donnie Van Zant, into a computer under the command center's triangular conference table. "We ordered this from Amazon last October. Okay, I put this in and it starts by default. Here's the EULA. Of course, I want to listen to the music, so I click 'Agree.'"

The player installs itself and launches automatically. Now Stahlberg chooses a guinea pig for the cloaking demonstration: the Windows calculator accessory. He starts the calculator, then opens the Windows Task Manager and selects the "Processes" tab, where a user can see a list of all of the programs currently running on the machine. "Okay, we can see it's there in the process list—it's called 'calc.exe.' Now let's rename it."

Stahlberg closes the calculator, finds the actual program file on the hard drive, and gives it a very specific name: "syscalc.exe." He restarts the calculator. "Now look at the process list again. The calculator has disappeared."

Stahlberg has just laid bare the main function of the Sony BMG rootkit: to make any file starting with the prefix "sys" undetectable. Among the files XCP keeps hidden in this way: aries, the ringleader program that waylays messages between applications and the operating system; cra-

Mika Stahlberg (left) and Santeri Kangas of data security firm F-Secure

MARKUS MARCETIC/MOMENT/REDUX

ter, the filter driver that keeps other programs from reading the CD-ROM; and sysparking, which counts how many times the burning application has been used.

"What almost all rootkits do…is filter the output that applications get from certain operating-system functions," Stahlberg explains. XCP filters out any output marked with the sys prefix, so in Stahlberg's demonstration, when the Task Manager asked Windows for a list of running programs, it got back everything except the calculator. A program with the sys prefix in its name may be running—indeed, it may be taking up a large fraction of the system's memory and CPU time—but to the Processes list and other applications such as Windows Explorer, it does not exist.

Of course, Stahlberg and his colleagues at F-Secure didn't understand any of this the first time they examined a copy-protected Sony BMG disc, Switchfoot's *Nothing Is Sound*. Immediately after receiving John Guarino's log file, they ordered the CD and installed it on a quarantined PC, then used F-Secure's own rootkit detection program, called Blacklight, to see how the disc's software had altered the machine's operating system. Blacklight found that there were more files in the system than Windows Explorer indicated—an unmistakable sign of a rootkit.

At first, the F-Secure researchers were reluctant to label the Sony BMG rootkit a security threat, since it was obviously being used for copy protection, not to spread viruses or spawn pop-up ads. "DRM as such is not bad", says Santeri Kangas, F-Secure's director of research. "But when we analyzed what this could do as a *vehicle* for malware, we took a stand and said, 'Well, this is dangerous.'"

F-Secure contacted Sony about the rootkit vulnerability on October 17. But the relationship got off to a bad start, according to Kangas. Not knowing whom to approach, F-Secure took the problem first to Sony DACD, an Austrian subsidiary that manufactures CDs. "They said, 'Thank you, but this is from Sony BMG,'" Kangas recounts. When he and his colleagues finally reached Sony BMG's Los Angeles headquarters, "The first reaction we got was, why were we talking about their copy protection software with a competing unit of Sony? They were rather angry."

Once the recriminations passed, Sony BMG DRM managers asked Kangas and his staff to work with First 4 Internet on a way to safeguard owners of the protected CDs. "From our point of view, the only solution with this first version of XCP was to stop deploying it," says Kangas. "But that was something they clearly didn't want to do." According to Kangas, First 4 Internet's plan was simply to release a new version of XCP in 2006 without the rootkit—not to replace the millions of discs that had already been purchased—and offer an uninstaller tool to customers who asked for it.

Kangas and his team readied a public report on the rootkit but were waiting for First 4 Internet's uninstaller before releasing it, as courtesy in the Internet security business demands. That's when they were beaten to the punch by a Texan named Mark Russinovich.

Russinovich and colleague Bryce Cogswell are the authors of Sysinternals.com, one of the leading U.S. blogs on computer security. Russinovich is also the chief software architect at Austin-based Winternals Software and, by chance, the inventor of some of the very cloaking techniques used by XCP. He and Cogswell had spent part of 2005 working on Rootkit Revealer, a detection program similar to F-Secure's Blacklight. One day in late October, Russinovich was running Rootkit Revealer on his own PC as part of a test to make sure the program wasn't generating false positives. Russinovich says he purposely avoids the seedier areas of the Internet in order to keep his machine clear of malware—so he was astonished when Rootkit Revealer found actual rootkit files.

Just as Guarino had, Russinovich discovered that deleting the files disabled his CD-ROM drive. "Even a sophisticated home user, if they attempted to uninstall the rootkit by deleting the files, would end up crippling their machine," Russinovich says. But since he had himself come up with most of the tricks Windows rootkits use to deceive the operating system and other applications, he wasn't stymied. Russinovich was able to bypass the rootkit's cloaking function and—after remembering that he'd recently played the copy-protected Sony BMG disc *Get Right with the Man* on his computer—trace the files it had been hiding to First 4 Internet and Sony BMG.

"It was disturbing to me, the fact that this thing had installed rootkit software on my PC," Russinovich says. "It had installed itself without telling me. There didn't appear to be any uninstaller. But what was most surprising of all was to run into a rootkit that was part of a well-known company's DRM."

Russinovich did not contact Sony BMG about his discovery; rather, he poured his findings into an angry blog entry published on Halloween. Within hours, Russinovich's post was picked up by Slashdot, the famous home of "News for Nerds." And from there the rootkit story raged across the blogosphere and even into mainstream newspapers. F-Secure—though it had been scooped by Russinovich—quickly got back into the game, publishing its own analysis of the rootkit on November 1.

Among music fans and technology watchers, reaction to the rootkit news was explosive. Within days, anti-DRM activists launched several boycotts against Sony BMG. "Sony aims at pirates—and hits users," blared a November 9 headline in the *Christian Science Monitor*. Antivirus and security companies issued warnings advising consumers to avoid or return the Sony BMG discs. Bloggers fanned the flames; the word "rootkit" appeared in blogs 150 to 750 times every day throughout November, according to blog search engine Technorati.

Tempers flared further after November 4, when Russinovich announced in his blog that other software accompanying XCP on the Sony BMG discs "phoned home," contacting Sony BMG over the Internet every time a user played a protected CD. Acting on a tip from a Finnish hacker and computer science student named Matti Nikki, Russinovich used a "network tracing" program to analyze traffic flowing into and out of his computer. He found that during startup, the protected CDs would check with a server at Sony BMG for fresh material for a rotating banner advertisement displayed with the player. This exchange was innocuous enough; but to Russinovich and readers of his blog, the affront was that Sony BMG had not disclosed in the CDs' EULAs that the software would send data to the company or spelled out how that data would be used. "I doubt Sony is doing anything with the data," Russinovich wrote, "but with this type of connection, their servers could record each time a copy-protected CD is played and the IP address [the location on the Internet] of the computer playing it."

Security professionals, bloggers, and music fans weren't the only ones who were dismayed. The U.S. Department of Homeland Security criticized Sony BMG for releasing products that undermined antivirus software and exposed both government-owned and privately owned computers to hackers. At a November 10 trade conference on piracy, Stewart Baker, the department's assistant secretary for policy, chastised big media for its obsession with DRM. "It's very important to remember that it's your intellectual property, [but] it's not your computer," Baker said.

Over and over again, people who encountered the rootkit expressed a sense of violation. John Guarino, the computer consultant, offers this analogy: "Say you want to install cable TV in your apartment. You call the cable company. They say someone is going to come and install it. The cable guy makes you sign something before he comes into the apartment. Then you find out he didn't actually leave the apartment when he was done. He is still hiding. And you call the company and say, 'This guy is still here,' and they say, 'But you signed the document.' And you say, 'Yeah, but he still shouldn't be here. Where is he?' and they say, 'We're not going to tell you that.'

"And not only is this guy hiding inside your apartment—he's actually eating from your refrigerator, drinking your water, using the bathroom, and you can't stop him. He could be inviting other friends over and letting them in. And if you try to find him and take him out yourself, he's going to throw bombs, and you'll have to call the construction guys to rebuild your whole apartment.

"That's what Sony is doing. The rootkit uses your processor, it uses your memory, your hard disk. You can't take

it out easily, because they won't tell you how. If you try to take it out, it actually messes up your computer. The only solution is to reinstall the whole operating system. It's total lawlessness, and it's unacceptable."

Facing the Music

Despite the warnings from F-Secure in late October, Sony BMG was surprised by the controversy. Indeed, for days after Russinovich's analysis hit the news, company executives showed little understanding of the fury it was arousing in the hearts of many of its customers. "Most people, I think, don't even know what a rootkit is, so why should they care about it?" Sony BMG's Hesse said in an interview with National Public Radio on November 4.

But for the owners of the more than two million XCP-protected discs sold by Sony BMG between January and November, the reports came as a shock. Security flaws in commercial software are common; Microsoft's products, for example, are so widely used that even the tiniest bug will eventually be discovered and exploited by a malware author, so the software giant publishes updates and patches on a monthly basis. But no software or media company of the stature of Sony BMG had ever distributed a program that, in the judgment of security experts, was deliberately designed to mimic malware.

"DRM as such is not bad," says Santeri Kangas of F-Secure. "But when we dug deeper and analyzed what this could do as a *vehicle* for malware, we took a stand and said, 'Well, this is dangerous.'"

Sony BMG did not immediately apologize but did try to solve the problem. Its first step, in early November, was to publish a Web-based program that customers could use to remove XCP from their systems. The move didn't help matters. Matti Nikki in Finland discovered that a file that the uninstaller placed on a user's computer to facilitate communication with Sony BMG's servers could later be exploited by any website that wanted to send and execute malicious code. The uninstaller posed "a far greater security risk than even the original Sony rootkit," according to Felten and Halderman, who verified Nikki's discovery on November 15 in their widely followed blog, Freedom to Tinker.

A few days later, Sony BMG replaced the Web-based uninstaller with a safer, downloadable one. And gradually, the company seemed to recognize the scope of the public-relations disaster it faced. On November 11, Sony BMG announced that it would stop manufacturing music CDs with XCP. On November 14, the company said it regretted the inconvenience it had caused its customers and announced an exchange program to replace XCP-protected discs with new ones without the rootkit.

According to media reports, consumers had purchased 2.1 million of the copy-protected CDs. How many of these customers actually played the CDs on their computers, thus unwittingly installing the rootkit, is not clear. But Dan Kaminsky, an independent security researcher in Seattle, discovered evidence linking Sony's rootkit to hundreds of thousands, if not millions, of systems across 131 countries. He calls that number "enormous," especially when compared with figures for the spread of Internet worms and viruses. Kaminsky posted the statistics on his website, doxpara.com, along with world maps showing the locations of affected networks.

Sony BMG, meanwhile, tried to respond to the specific worries raised by Russinovich, Kaminsky, and others. In a November 18 letter to the Electronic Frontier Foundation, which had earlier published its own open letter criticizing Sony BMG's handling of the XCP episode, Sony counsel Jeffrey Cunard said that the company would never disclose the Internet addresses collected when XCP phoned home and that, in any case, these addresses were never associated with personally identifiable information. He also said that Sony BMG would be more careful in the future about evaluating copy-protection software and the EULAs that come with it. "Any present and future copy protection technology used by Sony BMG will be tested, verified, and disclosed to consumers," Cunard wrote.

Sony BMG representatives contacted by *Technology Review* in March and April would not name the executives responsible for licensing XCP from First 4 Internet or releasing the copy-protected discs, and they declined to make executives available for interviews. However, Cory Shields, director of the company's communications office, said it was never Sony BMG's intention to include software that caused security concerns on its compact discs. "The company's intent was to deliver a technology that was consumer friendly, that would let people pursue the functionality that they wanted," Shields said. "It certainly wasn't the company's intent to create a problem."

Zone of Freedom

The recalls, exchanges, and apologies of November 2005 did not put the matter to rest. New York attorney general Eliot Spitzer criticized Sony in late November, after investigators found that discs carrying XCP had not yet been removed from stores. The Federal Trade Commission opened an inquiry,

and Texas attorney general Greg Abbott sued Sony BMG for violating the state's antispyware laws. Plaintiffs in at least five states filed suit, claiming damages against Sony BMG for impairing their computers.

Sony dealt with these suits quickly. Before December was out, the company had reached a tentative settlement with attorneys, who had consolidated the suits into a single complaint in the U.S. District Court for southern New York. The settlement provides anyone who owns a disc with XCP with a replacement disc, a $7.50 cash payment, and (ironically) free digital downloads of the music on the CD and up to three others. At press time, the court had not yet approved the full settlement, but the replacement program had begun.

But anger over the rootkit in the media and the blogosphere persisted even after news of the proposed settlement. What truly bothered consumers, it seemed, was not the damage done to their computers: the Troj/Stinx-E Trojan horse had not spread far, and there wasn't time for a serious epidemic of other malware exploiting the XCP rootkit to emerge. Rather, CD buyers were upset that the software deliberately concealed its presence and contacted Sony BMG without their permission. They felt that XCP had trespassed against fundamental protections—the rights to privacy and private ownership and the freedoms of expression and access to information.

Mark Russinovich

"I'm a music fan, and I've been watching with dismay the whole march of DRM, to the point that you practically have to sign a contract to open a CD box," says Tim Jarrett, a Framingham, MA, Web developer and technology blogger. "So when I saw that Sony was not only including this DRM but doing it in such a way that it was opening up people's computers to being exploited, I think something inside me just kind of snapped." Jarrett decided to start the Sony Boycott Blog, which functioned for three months as one of the main clearinghouses for information about the rootkit saga. Judging from the comments they left, Jarrett's readers—who numbered up to 5,000 per day—were just as irked. "You have a zone of personal freedom—a personal space within which you can decide, for example, to read a book back to front, or read it 20 times, or make margin notes, or read it in the bathtub, or do a skit acting out the book to a friend," says law professor Julie Cohen, who studies intellectual-property and data privacy law at the Georgetown University Law Center. "And having an automatic policeman or even just a flat-out architectural prohibition that appropriates that personal space is something that people experience as very intrusive."

"I think we're in this period where the content providers are trying to push the boundaries," says Mark Russinovich. "They want to see just how far they can go to protect their content, and where that fine line is between protecting their content from casual piracy and annoying the consumer."

Good DRM

The questions raised by the Sony BMG rootkit saga are whether protecting content necessarily means violating consumers' right to control their private property, compromising the computer's role as an instrument of culture and creativity, and sacrificing the principle of "fair use" (a provision in U.S. copyright law that allows the reproduction of copyrighted works for purposes of criticism, reporting, research, and archiving).

The initial signs are not good. Sony BMG's blunder—however inadvertent it may have been—was an indication to many observers that copyright holders are in fact escalating the technology war, choosing to meddle more and more deeply with the workings of customers' computers in a hasty and careless effort to limit freeloading.

"If Sony didn't stop and take the time to ask First 4 Internet what XCP actually did, it's their fault," says Schneier of Counterpane Internet Security. "I find First 4 Internet less culpable, because Sony wanted to buy some sort of magic bullet, and they just said, 'Here, use ours.'"

JOHN LANGFORD

Sony BMG has never fully accepted the blame; even in the December settlement agreement the company denied that it bore any legal liability or that anyone had been damaged by any wrongful conduct. Still, by most measures of corporate responsibility, Sony BMG has gone to remarkable lengths to make up for the rootkit fiasco. The company now seems to be wary of crossing Russinovich's "fine line." "There has to be a balance struck between protection of content and nurturing and protection of technology," acknowledges Sony BMG spokesman Cory Shields.

Indeed, Sony BMG's mistakes in the rootkit case provide some insights into what good digital rights management would, by contrast, look like.

First, say computer security professionals, good DRM should be *transparent*. To these professionals, the rootkit episode carried secrecy too far. If a rootkit provides a hiding place for viruses, worms, and Trojans, it makes the job faced by computers' virus-scanning software much more difficult. And if more legitimate companies start to design their software to mimic malware, that job becomes nearly impossible. "Now all of your security software has to distinguish between 'good' malicious code and 'bad' malicious code," Schneier says.

To be consumer friendly, therefore, DRM software must be computer friendly. It should not hide itself from the computer's operating system, nor take up more than its share of processing or memory. And the terms of use and functions of the software should be spelled out in a way that is clear to the user, not buried in a 20-page EULA. "People should understand the bargain they are making and the restrictions they may be subject to," says David Sohn, a staff counsel specializing in intellectual-property law at the Center for Democracy and Technology in Washington, DC.

Second, DRM technology should *respect users' privacy and security*. It should collect only that personal information needed for authentication, and only after obtaining the users' consent. And content protection measures cannot be implemented at the expense of a computer system's security against real malware.

Third, good DRM should be *user serviceable*. If a DRM system breaks, consumers should still be able to access the content they purchased, and if it becomes a secuity threat, they should be able to turn it off. Yet under the U.S. Digital Millennium Copyright Act (DMCA) of 1998, it is unlawful to circumvent the technology protecting digital content. There is no exception for cases such as that of the Sony BMG rootkit, where the DRM technology itself may be causing harm. This bizarre situation might be remedied if efforts by some lawmakers to amend the DMCA succeed. On December 14, for the third congressional session in a row, Rep. Zoe Lofgren, a Democrat from Silicon Valley, introduced a bill that would make it legal to circumvent DRM technology if the unprotected content is then used for noninfringing purposes, such as archiving. Lofgren's bill has been referred to the House Committee on the Judiciary, where it awaits review.

Fourth, and perhaps most important, good DRM technology should be *flexible*. The proposition Sony BMG made to customers with XCP was rather skimpy: buy this CD for $13.98 and you can make three copies, in Windows Media Audio format only. The copies can't be copied—and they won't play on other people's computers. Reasonable DRM, by contrast, would give consumers the freedom to use the content they've purchased in noninfringing ways, such as ripping it to their computers and uploading it to their mobile players, or perhaps let them choose exactly how they would like to use the content and charge accordingly. Time-shifting (recording live audio feeds for consumption later), place-shifting (streaming music over the Internet from a home computer to a remote location), or even sampling and remixing might all come with different price tags. "The marketplace should reward or punish products based on whether they are providing the flexibility people want," Sohn says.

Some DRM technologies offer increasing flexibility. Sohn points to FairPlay, the DRM system behind Apple's iTunes, as one example other content distributors might do well to imitate: customers can listen to FairPlay-protected songs on a computer, make playlists, burn those playlists to CDs, and move the songs to portable devices. (Sohn is not a fan of FairPlay's inability to operate with non-Apple products, however.) The success of the iTunes music store, Sohn says, suggests that this combination of features is "meeting consumer demand." TiVo to Go is another example: owners of TiVo digital video recorders can transfer recorded shows to DVDs, desktop PCs, laptops, and mobile devices such as the video iPod and Sony's PlayStation Portable.

But for every iTunes and TiVo, there are still numerous examples of restrictive DRM schemes that treat customers like criminals. Until there is consensus about what rights consumers deserve and which restrictions are necessary to protect the incomes of artists and their studios, buying digital content will probably continue to be a thorny business.

"There is absolutely a right for the holders of intellectual property to protect that property," says Stephen Toulouse, security program manager at the Microsoft Security Response Center, where researchers spent weeks last fall helping Windows users respond to the rootkit epidemic. "But as a consumer myself, I'd like to see software vendors and studios getting feedback from consumers and creating technologies that reflected it."

In the end, then, the record labels' best response to falling music revenues may be to exercise more imagination, not more control. TR

Wade Roush is senior editor at Technology Review.

By Emily Singer

Stem Cells Reborn

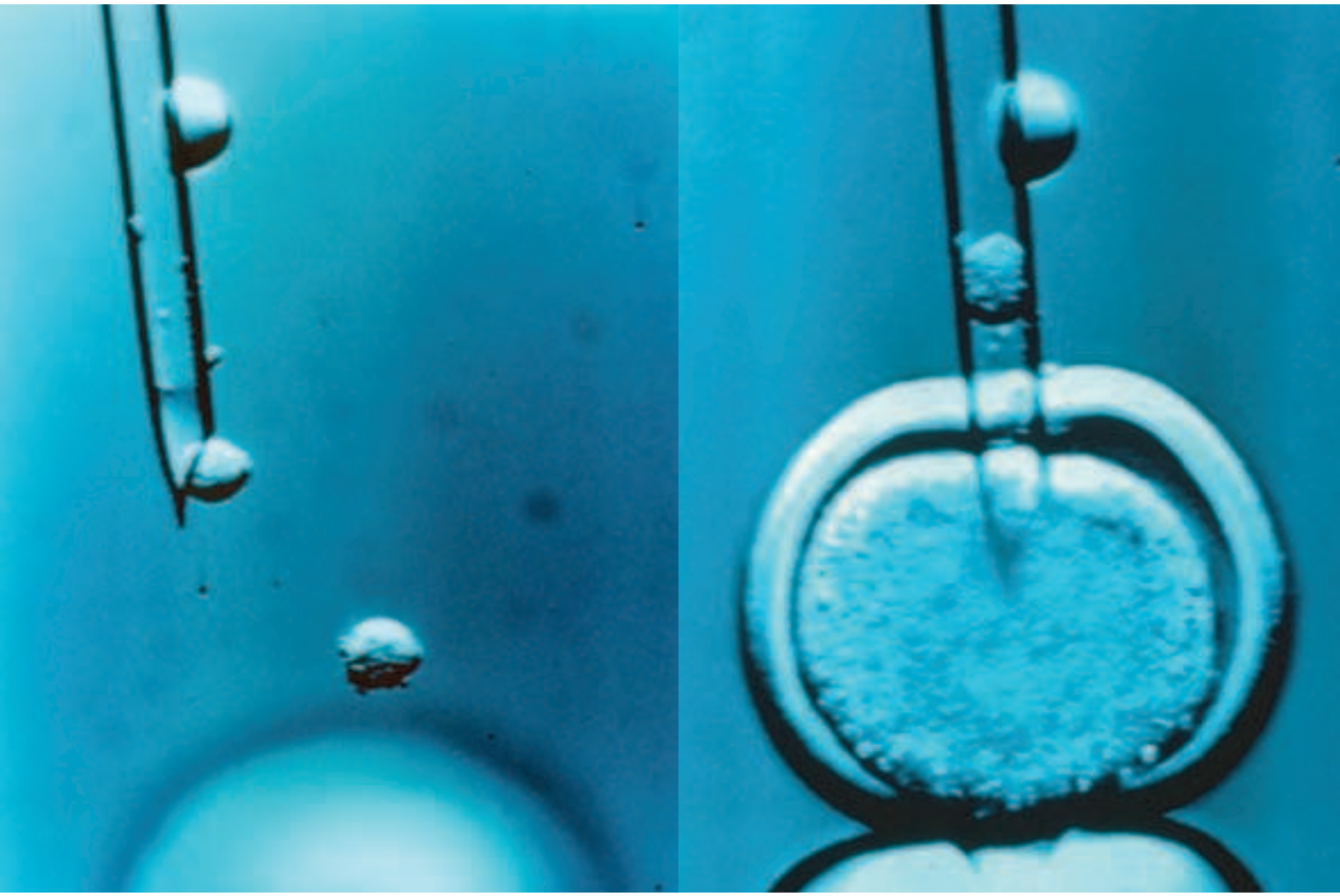
In the wake of devastating scientific fraud in South Korea, researchers are renewing their race to clone stem cells. Success could mean a new era of more-realistic disease models and safer, lifesaving regenerative medicine.

In late 2003, researchers at Advanced Cell Technology, a small biotech startup in Worcester, MA, thought they were about to do something remarkable. They had painstakingly generated cloned human embryos from adult cells and were trying to keep them alive long enough to harvest their inner cell masses, precious balls of cells that give rise to stem cells.

It was one of the most sought-after prizes of biomedical research: a way to grow embryonic stem cells directly from, say, a skin cell taken from a specific patient. It was also one of biomedicine's most speculative projects; indeed, the scientists at Advanced Cell Technology (ACT) were the only team in the United States actively pursuing it. But Robert Lanza *(see "Stem Cell Hope," p. 36)*, who headed the group, says he believes that his team at ACT was on the verge of success. If he's right, and if the work had continued, the company would almost certainly have had in its hands the key to a revolutionary new set of biomedical tools—and possibly to new treatments for a host of different diseases.

But in February 2004, the ACT scientists' hopes were dashed. A South Korean stem cell scientist named Hwang Woo Suk of Seoul National University and his colleagues announced in the journal *Science* that they had created patient-specific stem cells. The achievement vaulted Hwang to scientific stardom. His country named him its "supreme scientist" and honored him with a postage stamp depicting a paralyzed man able to walk again. Patients clamored to be part of his work. Hwang embraced his role as an international stem cell celebrity, announcing plans to create something called the World Stem Cell Hub, where members of his lab would clone and culture stem cell lines for scientists around the globe.

"What had been a terribly risky field that many scientists were loath to venture into now became a possibility," says Evan Snyder, director of the Stem Cells and Regeneration Program at the Burnham Institute for Medical Research in La Jolla, CA. Many U.S. researchers who had been unable or unwilling to start cloning work themselves began planning collaborations with the Korean scientists. "We knew



JAMES KING-HOLMES/PHOTO RESEARCHERS, INC.

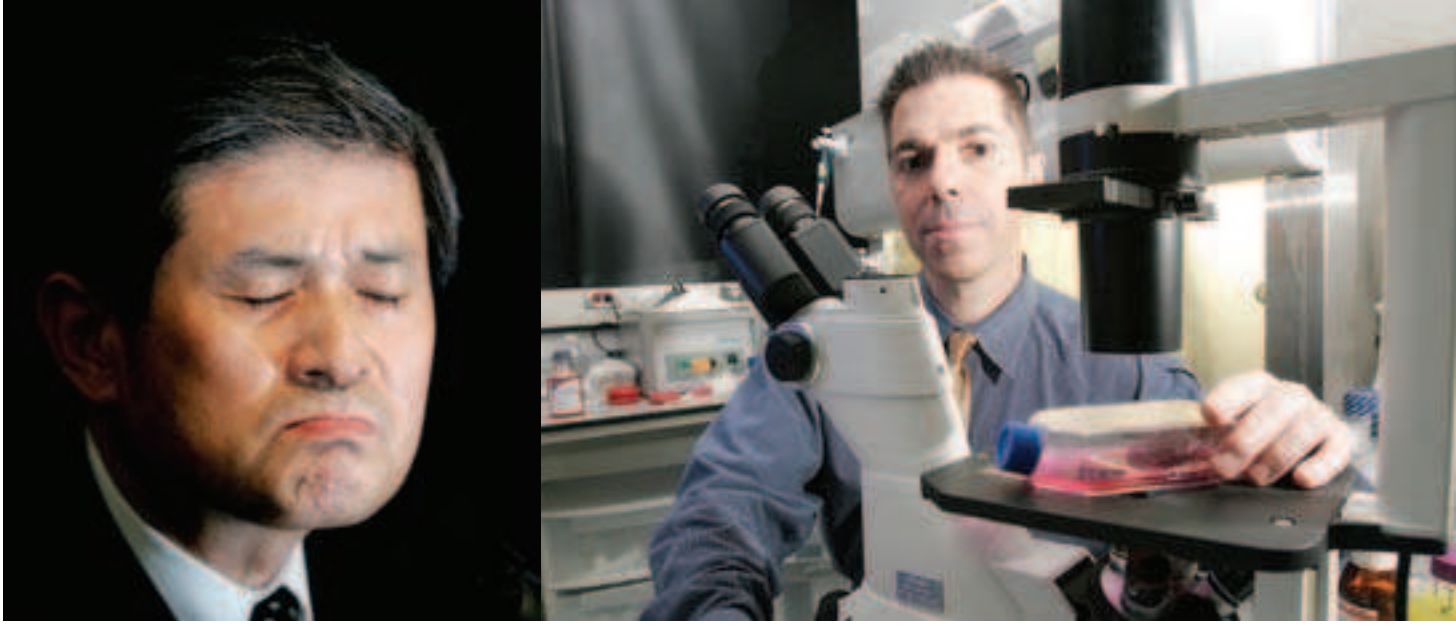
NUCLEAR TRANSFER **To create a cloned sheep embryo, scientists remove the nucleus from an egg (left). They then take a cell (middle) and insert it into the enucleated egg (above). Researchers hope to use similar technology to clone human stem cells.**

[cloning] would take a lot of time and money, and the Korean government was willing to throw so much at this one problem," says Snyder. "When that seemed to have been accomplished, many of us said, Well, that's a relief. Now we can do the real science experiments."

However, Lanza and his colleagues, who had been so close to cloning stem cells, watched dejectedly. "It was embarrassing," says Lanza. "This obscure group announced they had done it." ACT was already on shaky financial ground, but Hwang's achievement made its situation even more precarious. The company also abruptly lost its supply of human eggs—a crucial ingredient in cloning research—because clinics that ran donor programs felt no further need to participate in research whose central goal had been achieved. As a result, the scientists literally had to put their work on ice. "We had to freeze down lots of our cells. It shut down that research, and there has been no active research since," says Lanza. There was, plainly, no glory—or profits—in coming in second.

Only none of it was true. Beginning in May 2004, reports started trickling in that Hwang had used unethical means to obtain eggs for his cloning research and lied about it. By December 2005, it became clear that the deception was much more wide ranging. Hwang's human-cloning research, it seemed, was a spectacular fraud: investigators from Hwang's university found no evidence that his team had created cloned stem cell lines at all.

"It was like watching a car wreck taking place in slow motion. The magnitude of the problem was just really horrifying," says Snyder. "The world had been reset to pre-2004, like when Superman turned the world backwards. If you were pursuing cloning in 2004, you began pursuing it again. If you were sitting on the siddines, you were back sitting on the sidelines."



CLONING WOES **Robert Lanza (above), a stem cell scientist at Advanced Cell Technology, says that the fraudulent work of Hwang Woo Suk (left) at Seoul National University devastated his cloning program. Lanza hopes to start his research again soon.**

But some researchers couldn't turn back the clock. In the months since Hwang had made his announcement, ACT's investors had lost interest in producing patient-specific stem cells, and scientists at the company were now focusing on developing less risky stem cell therapies. "We were perceived as a failure, when in fact we were the furthest ahead," says Lanza, vice president of medical and scientific development at ACT. "We had lost a year of work and moved on to other things."

"The real work suffered because this guy was playing some game," Lanza continues. "I know I will be criticized for saying this, but I truly believe we had a protocol that would have been reproducible and straightforward, and we could have started on therapies by now."

Six months after the details of the fraud began emerging, Lanza and groups at Harvard University and the University of California, San Francisco, among others, are gearing up to start new programs to clone stem cells from adult donor cells—a process usually called somatic-cell nuclear transfer or therapeutic cloning. Despite the technical and political hurdles, the scientists are convinced that nuclear transfer will have a huge impact on medicine. Most immediately, they believe, cloned stem cells could be used as models in which to study human disease and test new drugs with unprecedented accuracy; eventually, stem cells could be transplanted directly into patients to cure degenerative diseases.

The Korean fraud, while clearly devastating for Lanza, may have inadvertently galvanized the field. "The Hwang episode was very destructive," says Ronald Green, an ethicist at Dartmouth College. "But Hwang's claims gave people a glimpse of what would be possible with cloned stem cells, and the consequence was a renewed interest in therapeutic cloning."

Scientists who had planned to collaborate with Hwang had spent months thinking seriously about what they could do with cloned stem cells, from creating new tools to shed light on the diseases they had studied for decades to investigating new treatments. The excitement those possibilities aroused, along with new influxes of cash from state and private sources, made many unwilling to wait on the sidelines any longer. Snyder, a pediatric neurologist and neonatologist who wants to develop new treatments for his patients, is now considering starting his own cloning program. "There is more of a readiness to get into this area, and I think that will carry over," he says.

Disease Payoff

In a freezer in La Jolla, CA, is a bank of frozen skin cells collected from patients with a rare and devastating genetic disorder called Lesch-Nyhan disease. Children born with the disease have a genetic error that causes them to produce too much uric acid, which builds up in their tissue. They also suffer major neurological problems in roughly the same part of the brain stricken by Parkinson's disease, resulting in motor and cognitive problems. "No one understands why a defect in this gene leads to a defect in the brain," says Theodore Friedmann, a pediatrician and geneticist at the University of California, San Diego, who has been studying the disease for almost 40 years.

About two years ago, Friedmann, an expert in gene therapy, began to consider how stem cells could help his patients. Embryonic stem cells have two valuable properties: under the right conditions, they can regenerate themselves—dividing to create identical new cells—and they are pluripotent, meaning they can develop into almost any type of cell in the body. That magnificent pliancy captivates scientists like Friedmann, who dream of the day they can take stem cells, coax them to become new brain or liver cells, and transplant them into patients with Parkinson's disease or organ failure.

Scientists have already shown that in animals, stem cells can help treat heart disease, spinal-cord injury, and sickle cell

KIM KYUNG-HOON/REUTERS/CORBIS (HWANG); RICK FRIEDMAN/WFPN (LANZA)

anemia, among other things. Rats with damaged spinal cords regained some mobility after injections of neural precursor cells made from embryonic stem cells. Stem cells transplanted into rats' heart tissue can help heal damaged heart muscles.

But before similar therapies can be tested in people, scientists will need to resolve the problem of immune rejection. Transplanted stem cells, which are now derived from discarded embryos, are genetically different from their recipients; like donor kidneys, they thus carry the risk of provoking an immune response. That means that even the most advanced treatments are still years away from clinical use. Therapeutic cloning is one way to make stem cells suitable for transplant, since it yields cells that share their recipients' DNA.

Theoretically, cloned stem cells could help Friedmann's patients; scientists could fix the genetic defect in the cells before implanting them. The prospect of such revolutionary treatment is what has most captivated both the public and the media. But Friedmann and Snyder are focusing on an application that could have much broader implications—and is closer at hand. Instead of using the cells as a form of therapy themselves, the researchers plan to use them to study Lesch-Nyhan disease and test new treatments. Experts say this type of application could dramatically improve our understanding of how any disease with a genetic component unfolds at the cellular level. "You could make a stem cell line that has ALS or Parkinson's, using DNA from a patient that really has the symptoms," says Snyder.

Scientists could prod the cells to develop into the type of cells damaged by a disease, such as dopamine neurons in Parkinson's, and study the intricate progression of the disease from its earliest stirrings to its final cellular death knell. Because the cells would be genetically identical to the patient's DNA, they would undergo many of the same molecular changes that underlie the patient's disease.

Ian Wilmut, the British scientist who helped clone Dolly the sheep, hopes to turn stem cells in a dish into motor neurons, the type of nerve cells ravaged in Lou Gehrig's disease (also known as amyotrophic lateral sclerosis, or ALS). Creating a stem cell line with the disease would allow scientists to study how these neurons sicken and die and to search for ways to slow or stop the downward spiral of the disease. "I think that disease models, such as the ones we plan to create, will do more in the short term, and maybe the long term, to treat disease than cloning stem cells for tissue transplants," Wilmut says.

One of the major advantages of cloned stem cells is that they would enable scientists to create accurate models of a disease without first determining the underlying genetics. "With a lot of sporadic diseases, we know there is a genetic component, but it's not clear what it is or how it contributes to the development of the disease," says Larry Goldstein, a neuroscientist at UCSD who studies Alzheimer's disease. "We have a lot of hypotheses, and I think this methodology will put us in a position to test those hypotheses. And if one is correct, we'll have a direction to go for therapy."

A stem cell model of Alzheimer's would also allow scientists to study what the disease does before symptoms appear and perhaps create early-diagnostic tests. By the time an Alzheimer's patient goes to the doctor with cognitive problems, the brain is significantly—and possibly irreversibly—damaged. "Studying the brains of people who have already died is like studying a plane crash after the plane hit the ground—you're looking at the wreckage," says Goldstein. "We want to look at the black box of Alzheimer's disease. What happens in those cells before the crash?"

> "The real work suffered because this guy was playing some game," Robert Lanza says. "I know I will be criticized for saying this, but I truly believe we had a protocol that would have been reproducible and straightforward, and we could have started on therapies by now."

To search for early signs of the disorder, scientists could generate stem cells using DNA from an Alzheimer's patient, then prod the cells to differentiate into neurons, monitoring them for the production of specific proteins or other molecular changes not seen in neurons derived from healthy embryonic stem cells. The same approach might work with cancer, which is characterized by a series of harmful genetic changes. "We want to know what's the earliest you can detect differences in disease cells," says Renee A. Reijo Pera, codirector of UCSF's human-embryonic-stem-cell biology program.

Cloned stem cells may also provide a much more effective way to test drugs. "Very often the animal models that exist for a particular disease really don't authentically replicate what's going on in a human," says Snyder. Using models based on stem cells, scientists could test drugs at different stages of disease, searching for compounds that could prevent a person at risk for, say, Alzheimer's, from ever developing the disease in the first place, or for compounds that stop or reverse the progression of damage in people who already have the disease.

Snyder eventually hopes to create stem cell models of many different neurodegenerative diseases. His first step,

in collaboration with Friedmann, will be to use the frozen skin cells housed at UCSD to create stem cells with Lesch-Nyhan disease. Snyder originally hoped Hwang would teach him the cloning process. But now the scientists plan to embark on the therapeutic-cloning project on their own and are working on getting regulatory approval and state or private funding.

Ethical Eggs?

To generate normal stem cell lines, scientists start with a fertilized embryo, usually discarded from an in vitro fertilization clinic. They collect a specialized ball of cells, called the inner cell mass, from the embryo when it is just five to six days old. Cultured in a dish, the cells develop into a line of embryonic stem cells that can, depending on the conditions, either regenerate itself or differentiate into specialized cell types, such as heart cells, liver cells, or brain cells. Scientists must continually make new stem cell lines, because existing lines may accumulate mutations, making them unfit for therapies and many types of research.

Cloned stem cells, however, are even more difficult to make than regular embryonic stem cells. Scientists take the DNA from a differentiated cell, such as a skin cell, and insert it into an egg that has been stripped of its own DNA. The egg then starts dividing, much as a regular embryo would. If it survives long enough, its inner cell mass can be harvested and used to grow stem cells. Scientists have generated stem cells from cloned mouse embryos but have not replicated that feat in humans. Unlike naturally fertilized embryos, cloned embryos are hard to keep alive long enough—almost a week—that their inner cell masses can be gathered.

Hwang had claimed to do this with remarkable efficiency, using a small number of eggs. Human eggs are a precious resource that is very difficult to obtain, so the frugal use of eggs is critical to making nuclear transfer practical. But subsequent investigations revealed that Hwang and colleagues lied not only about their results but also about the number of eggs they used in their experiments. According to a report from South Korea's National Bioethics Committee, Hwang used 2,221 eggs in his failed experiments, rather than the 427 eggs reported in his two *Science* papers. Scientists now have no idea how many eggs are required to successfully clone a line of human stem cells.

When the nucleus of an adult cell is put into an egg, some unknown factors in the egg turn back the clock on it, reverting it to its embryonic state. "It's like pushing the reformat key on a computer. You reformat it to become some other kind of cell," says Snyder. "We don't understand the molecular pathways that do this....As far as we know, the only thing that can do this is the egg"

According to Kevin Eggan, a molecular and cellular biologist at Harvard who is seeking approval from his university to start nuclear-transfer research, "It's not clear how many eggs we need or how many women will step forward to donate eggs." Eggan, who also sits on the ethics review board of the California Institute for Regenerative Medicine (and was a member of the 2005 TR35), says he's spent much of the last year learning about the ethical and medical issues associated with egg donation. Many scientists say access to eggs will determine the success of therapeutic cloning. "We have a therapy that could have revolutionized medicine like antibiotics, but we have a bottleneck that shoots it down," says Lanza.

The egg donation procedure is uncomfortable and potentially painful and carries some medical risk. Women must undergo hormone treatments to stimulate ovulation, counseling sessions to understand the risks involved, and a medical procedure in which a needle is inserted into the vagina to remove eggs from the ovary. A small percentage of donors develop ovarian-hyperstimulation syndrome, which in rare cases can cause kidney failure.

Even ardent supporters disagree over the most ethical ways to handle egg donation. Some scientists don't want to use human eggs at all. "We feel it's inappropriate to put women through a risky and potentially dangerous procedure when we don't know what the efficiency is," says Stephen Minger, a scientist at King's College London who is planning to apply for permission from the British government to clone human stem cells using animal eggs. Those who do want to use human eggs disagree about whether women should be paid for their donations. Opponents worry that payment could encourage some women to undergo the procedure without understanding the risks. But others think compensation is the most ethical approach. "When ACT did this, we paid egg donors," says Green. "I continue to think that's the best way to do it. It's fair and open and the least likely to lead to evasion."

According to Lanza, all the women who recently contacted ACT about donating eggs dropped out of the process when they learned how much time was involved. Lanza says he still plans to proceed, as soon as he can get a new source of eggs. "If I were just starting, I probably wouldn't do it," he says. "Sometimes I spend more time on the phone with lawyers than I do on the science....But we've invested so much time and energy and so much of ourselves that we want to see this to completion. I still feel there is a very important role for [nuclear transfer] in different diseases."

Lanza suspects that, because of the shortage of eggs and the unknown efficiency of the cloning process, the therapeutic use of cloned stem cells will end up looking more like a kidney transplant than like the ingestion of a widely prescribed drug. "We do recognize it's not the broad cure we had hoped, but I'm convinced it will save some individuals," he says. "Perhaps a mother would donate a round of eggs to create stem cells for her sick child."

Federal Blockage

As American scientists gear up for the new race toward nuclear transfer, they face many of the same hurdles that stranded most of them in the starting block two years ago. Hwang had huge sums of money from the Korean government, an adoring public, and an enormous, albeit ethically unsound, supply of human eggs. U.S. scientists face intense public scrutiny, an administration opposed to embryonic-stem-cell research, and a continuous struggle to get funding from private investors.

In 2001, President Bush limited federal funding for embryonic-stem-cell research to work involving a small number of cell lines already in existence. That policy has exerted a disastrously chilling effect on the field. Scientists who wish to do research on newly derived embryonic-stem-cell lines or to derive new lines themselves—as is necessary in nuclear transfer—must find private sources of funding.

Scientists and university administrators also face the arduous task of separating all publicly and privately funded research. "It means everyone is dragging 10-pound weights on their feet," says Greg Simon, president of FasterCures, a Washington, DC–based advocacy group that aims to speed development of novel therapies. "We're spending a lot of wasted time separating government money from private money when we should be spending time doing research."

The federal blockade also means that the National Institutes of Health, the nation's largest biomedical-research institute, has forsaken its standard regulatory role, leaving many scientists operating in a vacuum. The National Academy of Sciences has tried to pick up some of the slack, publishing a nonbinding set of guidelines for stem cell research in 2005 and creating a stem cell research oversight committee earlier this year.

Many state governments have felt compelled to step in, both regulating and providing funding for stem cell research. So far, California, Connecticut, Massachusetts, and New Jersey have passed laws that permit embryonic-stem-cell research, including work on cloned embryos. Arkansas, Indiana, Iowa, Michigan, North Dakota, and South Dakota prohibit research on cloned embryos.

In addition, California, Connecticut, and New Jersey have all earmarked state funds to support stem cell research not funded by the federal government. The California initiative, by far the biggest at $3 billion, has encountered pitfalls at every turn, demonstrating the difficulties that arise when states get into the research-funding business. The California Institute for Regenerative Medicine, the oversight entity created by the state's Proposition 71, has grappled with accusations of conflicts of interest among those who determine the distribution of funds and with controversies over how the state will reap the financial benefits of stem cell research—a promise that was part of the proposition.

Overcoming Immunity

One of the biggest obstacles to stem cell–based therapies is the possibility of immune rejection, as can happen with donor kidneys. Patient-matched stem cells—derived from a patient-donated skin cell—could present a way around this problem. But as researchers have come to believe that cloning stem cells may be too inefficient for broad use, they have begun developing other ways to overcome immune rejection.

Rather than creating stem cell lines for every patient who needs them, says Stephen Minger, a stem cell scientist at King's College London, we might do better to create 1,000 stem cell lines representing the most common immune profiles in the population. "You wouldn't get a perfect match for everyone…but you would be close, and you might only need mild immunosuppression," he says.

Scientists are also developing ways to use stem cells to deceive the immune system. "If you can knock out [immune response], it's possible you can have cells sneak under the radar," says Tim Kamp, a stem cell scientist at the University of Wisconsin–Madison. Preliminary research suggests that turning stem cells into a type of immune cell known as a dendritic cell can trick the host's immune system into accepting other, related cells. If scientists made both immune cells and whatever cell type was needed for therapy from the same lines of stem cells, they might be able to inject both cell types into a patient without an immune response.

In some cases, doctors may not need to worry about immune rejection. "We're starting to recognize that stem cells may be better tolerated by the immune system in some areas of the body than we expected," says Evan Snyder, a neurologist at the Burnham Institute in La Jolla, CA. "Embryonic stem cells seem to be tolerated in the brain, even without immunosuppression."

Geron, a California-based biotechnology company developing embryonic-stem-cell therapies, is taking advantage of this fact to develop new treatments for spinal-cord injury. Scientists have spurred injured rats to walk again after injections of neural precursor cells derived from embryonic stem cells; Geron is seeking permission to start human clinical trials of a related procedure next year.

Almost all embryonic-stem-cell research in the United States faces funding obstacles and ethical objections, but because nuclear transfer is the most contentious topic in the field—it involves not only the destruction but also the *creation* of embryos specifically for research—scientists and universities planning nuclear-transfer programs are extracautious. "The spotlight is on anyone doing this kind of research," says Lanza. For example, Massachusetts law mandates criminal penalties for people who violate laws governing egg and embryo procurement. "If we slip up anywhere, we'll be crucified," Lanza says.

Other countries have much more supportive environments for embryonic-stem-cell research, which may give them the lead in the new race to perfect nuclear transfer. In the United Kingdom, for example, stem cell research is more intensely regulated but also much more open. Scientists apply to a central government authority for permission to do research involving human embryos. Summaries of research proposals under review—including those involving nuclear transfer—are posted online for public evaluation, along with an explanation of the criteria for approval. "In the U.K., we have enormous government support, from the prime minister on down," says Minger, an American scientist who migrated to the UK. "There's a stigma associated with stem cells in the U.S. that's not true here."

This openness contrasts with the situation at Harvard, where several scientists applied for permission to do nuclear-transfer research more than two years ago. According to Massachusetts state law, the researchers must get their experiments approved by institutional review boards. But whereas the British approval procedure is largely transparent, neither Harvard officials nor scientists proposing experiments would discuss with *Technology Review* their research plans or the details of the review process until after it is completed.

"In the U.K., we have enormous government support, from the prime minister on down," says Stephen Minger. "There's a stigma associated with stem cells in the U.S. that's not true here."

Across the Atlantic, government support has helped two U.K. groups charge to the forefront of therapeutic-cloning research. Alison Murdoch, Miodrag Stojkovic, and collaborators at the University of Newcastle upon Tyne have probably made more progress in nuclear transfer than any other researchers. Murdoch's team received permission from the U.K. authority to start experiments in August 2004 and announced that it had cloned an early-stage embryo (it hasn't yet isolated stem cells) soon after Hwang published his now retracted paper announcing an efficient cloning technology. At the University of Edinburgh, Wilmut also intends to do nuclear transfer. He put his plans on hold after the Hwang scandal, but he is now seeking permission to start a new set of experiments, using animal eggs rather than human eggs.

California's Haven

In a lab high on a hill overlooking the San Francisco Bay, Renee Reijo Pera sits at her desk listening to the sounds of construction. The space next to her lab has been entirely gutted; ladders and scattered extension cords have replaced the orderly rows of microscopes and freezers. Upon completion in August, the space will become the home of UCSF's new therapeutic-cloning research program. It will effectively be a replica of Reijo Pera's current lab, stocked with the same sort of equipment, but purchased with private funds.

UCSF hopes the new facility will help it become a frontrunner in therapeutic cloning. The university was the first in the United States to attempt nuclear transfer, albeit unsuccessfully, in the 1990s. "Now we hope to start again where those studies left off," says Arnold Kriegstein, director of the university's Institute for Stem Cell and Tissue Biology.

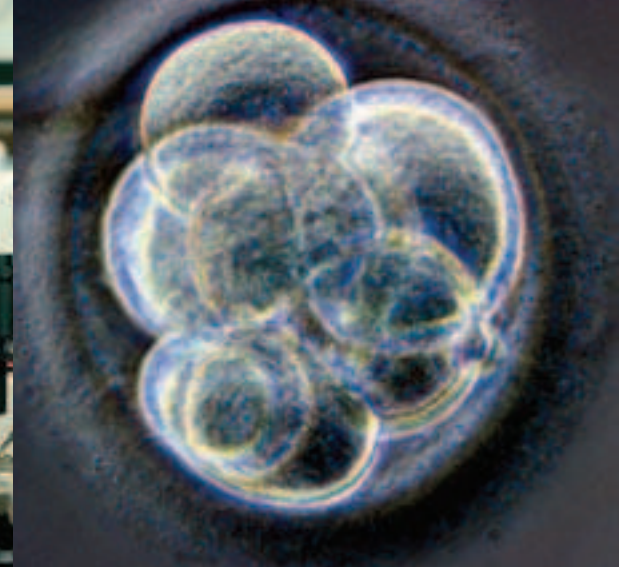
Reijo Pera and colleagues started cloning experiments at another off-site facility in April, possibly the first U.S. group to try human nuclear transfer since Lanza's team halted its work in 2004. In the UCSF lab, they will use "fail to fertilize" eggs from an in vitro fertilization clinic, which are much easier to get than donor human eggs. When they have optimized the experimental conditions, they will start using human eggs donated specifically for research.

UCSF's new program is just one sign of California's bid to become a haven for therapeutic cloning. The $3 billion in state funding for stem cell research that voters approved in 2004 has been held up in legal disputes; but in the interim, the oversight agency is issuing bonds to raise money for stem cell programs. Many universities that hope to receive some of that money say that nuclear transfer will be a major part of their research agendas.

Two teams of scientists at Harvard with an impressive dossier also plan to start nuclear-transfer experiments. George Daley at Children's Hospital Boston wants to create patient-matched stem cells for bone marrow transplants for children with blood diseases, such as leukemia. Currently, many of these children cannot find donors whose bone marrow is a close enough match to be suitable for transplant. And sometimes even matched bone marrow transplants can trigger a severe immune reaction. Eggan, an expert in mouse cloning, and Doug Melton, a molecular and cellular biologist at Harvard, want to use cloning to create new models of neurodegenerative disease and diabetes. The Harvard scientists hope to get final approval for their respective projects this year.

Reprogramming the Debate

Tobias Brambrink sits at a microscope, staring at a plate coated with millions of specialized skin cells known as fibroblasts. He hopes to find a clump of cells that glow green, or even better, some cells that have the rounded shape of stem cells, rather than the elongated shape of fibroblasts.



U.K. FRONTRUNNERS **In 2005, Miodrag Stojkovic and Alison Murdoch (left) at the University of Newcastle upon Tyne announced they had created an early-stage cloned human embryo (above).**

Brambrink, a postdoctoral researcher in Rudolf Jaenisch's lab at the Whitehead Institute for Biomedical Research in Cambridge, MA, is searching for the genetic switches that control reprogramming—a poorly understood transformation that takes place during cloning, reverting an adult cell to its embryonic state.

All cells in an organism share the same genes, but the pattern of a cell's gene activity determines whether it will become a stem cell or a differentiated cell. During reprogramming, some still-unknown factors in the egg turn off the genes that make a cell, say, a neuron and turn on the genes that are expressed in embryos. To uncover the genes controlling this conversion, Brambrink has engineered adult cells to express the genes that are selectively activated in eggs. If a particular gene expressed by one of these cells is crucial to the reprogramming process, it will activate genes that are known to be involved in the process's later stages; those genes have been tagged with markers that make the cell glow green. In the best-case scenario, the activator gene might trigger reprogramming itself, creating a clump of stem cells where once sat differentiated fibroblasts.

Reprogramming cells in a dish would be a huge breakthrough for the field of therapeutic cloning. Once scientists understand the process, they can create new technologies to turn adult cells directly into stem cells. Such technologies would eliminate the ethical controversy surrounding embryonic stem cells, because they would not require the creation and destruction of human embryos. They would also eliminate the need for human eggs, which could make therapeutic cloning much more efficient and therefore more broadly useful. Such an advance could truly usher in a new era of regenerative medicine, where a tailored stem cell transplant is available to anyone who needs one.

Scientists have already shed some light on the reprogramming process. In a paper published in September, Rick Young, a biologist at Whitehead, and colleagues identified a set of genes that are kept inactive in undifferentiated stem cells. Researchers theorize that when these genes are turned on, they produce transcription factors that spur the cells along different developmental paths.

Scientists caution that a clear picture of reprogramming—one that would enable the production of stem cells without eggs—is likely decades away. However, the little known so far is already helping scientists develop new, less controversial techniques for creating stem cells. For example, scientists are searching for ways to create genetically altered embryos that no longer have the potential to develop into human beings, thus eliminating some of the ethical controversy surrounding nuclear-transfer research. Markus Grompe, director of the Oregon Stem Cell Center at Oregon Health and Science University in Portland, hopes to create such a technology by forcing donor cells to express genes normally found only in embryonic stem cells *(see "10 Emerging Technologies: Nuclear Reprogramming," March/April 2006)*.

In fact, nuclear transfer may turn out to be a transitional technology. But even if it is, and for all its controversy, it might still be vitally important as the key to developing newer technologies that are able to finally free embryonic stem cells from ethical quandaries. "Nuclear transfer is the only way we can currently do reprogramming. This is our model and our yardstick to learn what's important," says Whitehead's Jaenisch. Adds Snyder, "If we don't know how to do nuclear transfer, or we're not allowed to do it, then this potentially debate-solving technique becomes impossible to pursue."

Lanza is also working on new reprogramming technologies to get around the shortage of eggs. But like Snyder, he worries that too much focus on uncertain alternatives could derail progress on therapeutic cloning, which scientists know works. "Let's develop all these technologies and see what works best," he suggests. He adds that months and years of grappling with the ethical and legal issues surrounding stem cell research, rather than the science, have worn him down. But the thought of stem cell–based therapies pushes him to keep going. "I've often gone home and thrown up my hands. But then I say, We can't give up that easily." TR

Emily Singer is the biotechnology editor of Technology Review.

CRAIG CONNOR/NORTH NEWS & PICTURES/REUTERS/CORBIS (RESEARCHERS); RBM ONLINE/REUTERS/CORBIS (EMBRYO)

Tiny Toxins?

Preliminary studies suggest that some types of nanoparticles might pose a health hazard. If so, it could throw a shadow over the nanotech revolution.

By Philip E. Ross Illustration by Jason Holley

It was just the type of event that many in the nanotechnology community have feared—and warned against. In late March, six people went to the hospital with serious (but nonfatal) respiratory problems after using a German household cleaning product called Magic Nano. Though it was unclear at the time what had caused the illnesses—and even whether the aerosol cleaner contained any nanoparticles—the events reignited the debate over the safety of consumer products that use nanotechnology.

The number of products fitting that description has now topped 200, according to a survey published in March by the Project on Emerging Nanotechnologies in Washington, DC. Among them are additives that catalyze combustion in diesel fuel, polymers used in vehicles, high-strength materials for tennis rackets and golf clubs, treated stain-resistant fabrics, and cosmetics. These products incorporate everything from buckyballs—soccer ball–shaped carbon molecules named after Buckminster Fuller—to less exotic materials such as nanoparticles of zinc oxide. But they all have one thing in common: their "nano" components have not undergone thorough safety tests.

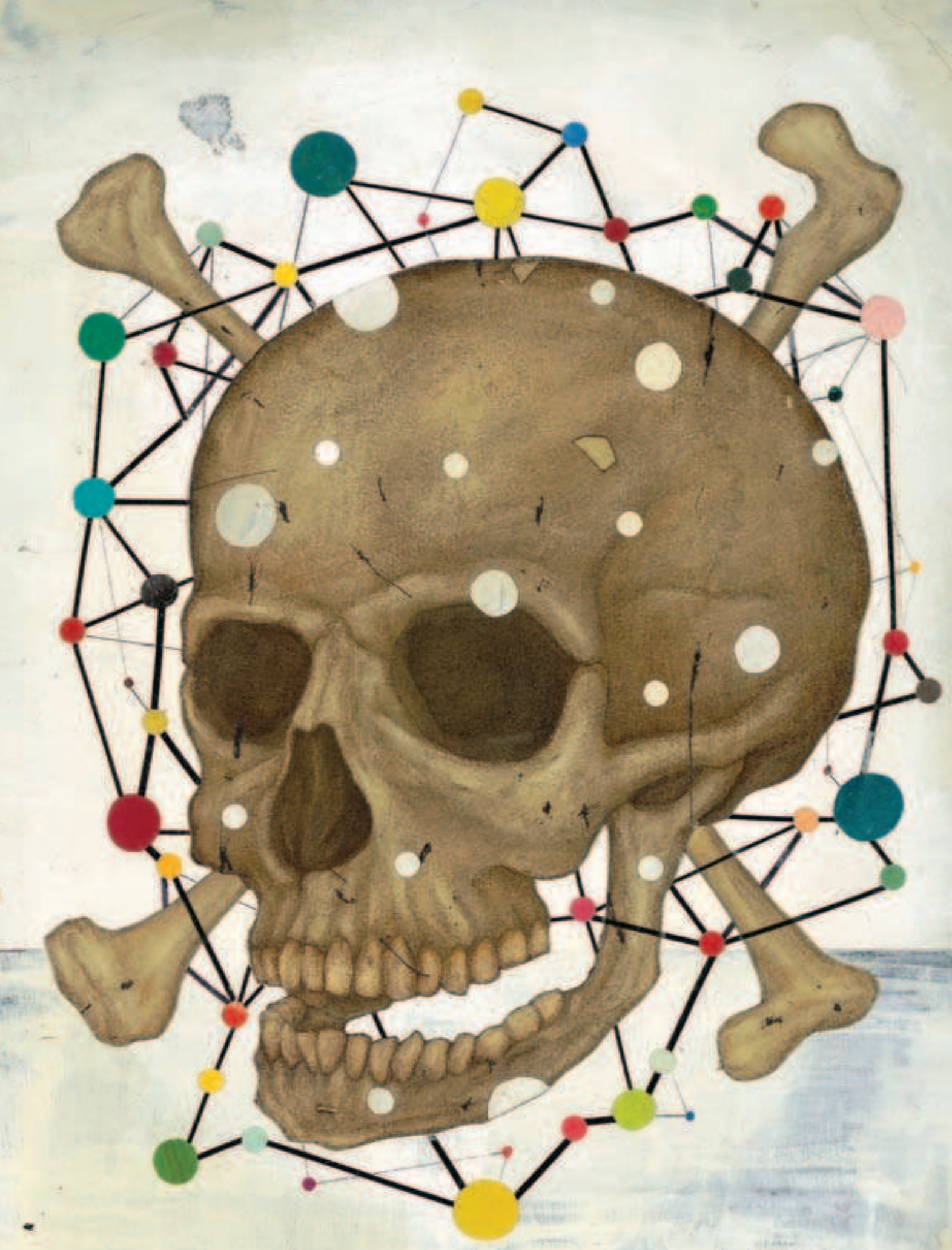
Nanoparticles, which are less than 100 nanometers in size, have long been familiar as by-products of combustion or constituents of air pollution; but increasingly, researchers are designing and synthesizing ultrasmall particles to take advantage of their novel properties. Most toxicologists agree that nanoparticles are neither uniformly dangerous nor uniformly safe, but that the chemical and physical properties that make them potentially valuable may also make their toxicities differ from those of the same materials in bulk form.

One of the reasons for concern about nanoparticles' toxicity has to do with simple physics. For instance, as a particle shrinks, the ratio of its surface area to its mass rises. A material that's seemingly inert in bulk thus has a larger surface area as a collection of nanoparticles, which can lead to greater reactivity. For certain applications, this is an advantage; but it can also mean greater toxicity. "The normal measure of toxicity is the mass of the toxin, but with nanomaterials, you need a whole different set of metrics," says Vicki Colvin, a professor of chemistry at Rice University in Houston and a leading expert on nanomaterials.

Beyond the question of increased reactivity, the sheer tininess of nanoparticles is itself a cause for concern. Toxicologists have known for years that relatively small particles could create health problems when inhaled. Researchers have found evidence that the smaller particles are, the more easily they can get past the mucus membranes in the nose and bronchial tubes to lodge in the alveoli, the tiny sacs in the lungs where carbon dioxide in the blood is exchanged for oxygen. In the alveoli, the particles face the white-cell scavengers known as macrophages, which engulf them and clear them from the body. But at high doses, the particles overload the clearance mechanisms.

It is the potential growth, however, of technologies involving precisely engineered nanoparticles, such as buckyballs and their near cousins, carbon nanotubes, and the use of these new materials in consumer products that has made the question of toxicity particularly urgent.

In addition to questions about how easily nanoparticles can penetrate the body, there is also debate over where they could end up once inside. Günter Oberdörster, a toxicologist at the University of Rochester, found that various kinds of carbon nanoparticles, averaging 30 to 35 nanometers in diameter, could enter the olfactory nerve in rodents and climb all the way up to the brain. "There is a possibility that because



of their small size, nanoparticles can reach sites in the body that large particles cannot, cross barriers, and react," says Oberdörster.

In 2004, Oberdörster's daughter, Eva Oberdörster, a toxicology researcher at Duke University, put largemouth bass into water containing buckyballs at the concentration of one part per million. After two days, the lipids in the brains of the fish showed 17 times as much oxidative damage as those of unexposed fish.

Carbon nanotubes, which are basically cylindrical versions of the spherical buckyballs, are one of the stars of nanotech, with potential uses in everything from solar cells to computer chips. But in 2003, researchers at NASA's Johnson Space Center in Houston, headed by Chiu-Wing Lam, showed that in the lungs of mice, carbon nanotubes caused lesions that got progressively worse over time. Under the conditions of the experiment, the researchers concluded, carbon nanotubes were "much more toxic than carbon black [that is, soot] and can be more toxic than quartz, which is considered a serious occupational health hazard."

Another extremely promising nanoparticle is the fluorescent "quantum dot," now being explored for use in bioimaging. Researchers envision applications in which they tag the glowing nanodots with antibodies, inject them into subjects, and watch as they selectively highlight certain tissues or, say, tumors. Quantum dots are typically made of

Mixed Findings on Toxicity

Group	Key findings	Caveat	Reference
David Warheit, DuPont Haskell Laboratory (2004)	Instilling nanotubes in the lungs of rats can cause adverse reactions.	Not a realistic model of exposure: the study had no findings on the effects of rats' inhaling nanoparticles.	"Comparative Pulmonary Toxicity Assessment of Single-Wall Carbon Nanotubes in Rats," *Toxicological Sciences* 77: 117–125
Günter Oberdörster, University of Rochester (2004)	Inhaled nanoscale particles can get into rats' brains via the olfactory nerve.	Results might not apply to humans. The study did not demonstrate toxicity or study common manufactured nanoparticles.	"Translocation of Inhaled Ultrafine Particles to the Brain," *Inhalation Toxicology* 16(6–7): 437–445
Eva Oberdörster, Duke University (2004)	Fullerenes can damage cells in the brains of fish by increasing peroxidation.	Cells in the gills and liver showed decreased peroxidation after exposure to fullerenes, for undetermined reasons.	"Manufactured Nanomaterials (Fullerenes, C_{60}) Induce Oxidative Stress in the Brain of Juvenile Largemouth Bass," *Environmental Health Perspectives* 112: 1058–1062
Daniel Watts, New Jersey Institute of Technology (2005)	Nanoscale alumina can stunt root growth in corn, soybeans, and other plants, suggesting nanoparticles can be toxic to plants as well as animals.	Chemically altering the surfaces of the particles dramatically reduced their toxicity.	"Particle Surface Characteristics May Play an Important Role in Phytotoxicity of Alumina Nanoparticles," *Toxicology Letters* 158: 122–132
Joseph Hughes, Georgia Institute of Technology (2005)	Fullerenes can damage microbes. (This study and the next elucidate the mechanisms of toxicity and may help scientists predict the effects of a range of nanoparticles.)	The study models just one aspect of how nanoparticles will interact with the environment.	"C_{60} in Water: Nanocrystal Formation and Microbial Response," *Environmental Science and Technology* 39: 4307–4316
Jennifer West and Vicki Colvin, Rice University (2005)	In human cells, fullerenes can cause damage like that seen in the brain cells of fish.	Particles may behave differently in the body than they do in cell cultures.	"Nano-C_{60} Cytotoxicity Is Due to Lipid Peroxidation," *Biomaterials* 26: 7587–7595
Kevin Ausman and Vicki Colvin, Rice University (2006)	Modifying the surfaces of carbon nanotubes with functional molecules can increase their toxicity.	Functionalizing nanoparticles can negate the very properties that make them useful for some applications.	"Functionalization Density Dependence of Single-Walled Carbon Nanotubes Cytotoxicity in Vitro," *Toxicology Letters* 161: 135–142

cadmium selenide, which can be toxic as a bulk material, so researchers encase them in a protective coating. But it is not yet known whether the dots will linger in the body, or whether the coating will degrade, releasing its cargo.

Sensible regulation of nanoparticles will require new methods for assessing toxicity, which take into account the qualitative differences between nanoparticles and other regulated chemicals. Preferably, those methods will be generally applicable to a wide spectrum of materials.

Today's assays are not adequate for the purpose, says Oberdörster. "We have to formalize a tiered approach," he says, "beginning with noncellular studies to determine the reactivity of particles, then moving on to in vitro cellular studies, and finally in vivo studies in animals. We have to establish that some particles are benign and others are reactive, then benchmark new particles against them."

Separately testing every newly developed type of nanoparticle would be a Herculean task, so Rice's Colvin wants to develop a model that indicates whether a particular nanoparticle deserves special screening. "My dream is that there would be a predictive algorithm that would say, for a certain size and surface coating, this particular type of material is one you'd want to stay away from," she says. "We should be able to do it, with the advance we have made in computing power, but we have to ask the right questions. For instance, is it acute cytotoxicity, or is it something else?"

Amidst all the uncertainty about evaluating nanoparticles' toxicity, regulatory agencies are in something of a quandary. In the United States, the Food and Drug Administration will assess medical products that incorporate nanoparticles, such as the quantum dots now being tested in animals; the Occupational Safety and Health Administration is responsible for the workplace environment in the factories that make the products involving nanoparticles; and the Environmental Protection Agency looks at products or chemicals that broadly permeate the environment, like additives to diesel fuel. In principle, these federal agencies have sweeping power over nanomaterials, but at the moment, their traditional focus, their limited resources, and the sheer lack of test tube and clinical data make effective oversight next to impossible.

For example, the National Institute for Occupational Safety and Health, the part of the Centers for Disease Control and Prevention in Atlanta responsible for studying and tracking workplace safety, acknowledges that "minimal information" is available on the health risks of making nanomaterials. The agency also points out that there are no reliable figures on the number of workers exposed to engineered nanomaterials.

The EPA seems further along. In its draft "Nanotechnology White Paper," issued in December, it proposed interagency negotiations to hammer out standards and pool resources. It acknowledged that at present, some nanoparticles that should be under its review are not, because they are not included in the inventory of chemicals controlled under the Toxic Substances Control Act.

The EPA must defend the safety not only of human beings but of the natural environment—plants and ecological systems that may be exposed to a regulated material. There is scant data on the effects of nanomaterials in the environment, but some of it is troubling. One study, for example, showed that alumina nanoparticles, which are already commonly used, inhibit root growth in some plants.

In a report written for the Project on Emerging Technologies, J. Clarence Davies, assistant administrator for policy, planning, and evaluation at the EPA from 1989 to 1991, advocates passing a new law assigning responsibility for nanomaterial regulation to a single interagency regulatory authority. Davies would also require manufacturers to prove their nanotech products safe until enough evidence had been gained to warrant exemptions.

But some executives in the nanotech industry cringe at the prospect of such regulations. Alan Gotcher, head of Altair Nanotechnologies, a manufacturer in Reno, NV, that makes various types of nanoparticles, testified before the U.S. Senate in February and cited the Davies report. "To fall into 'a one-size-fits-all' approach to nanotechnology," he said, "is irresponsible and counterproductive." Gotcher would prefer a government-funded effort to amass the necessary data and build the necessary models before setting any standards.

It is doubtful, however, that the nanotech community will stop developing new products, or that the public will stop buying them, while awaiting a new regulatory framework that could take years and millions of dollars to finalize. While few agree on how to efficiently determine the toxicity of nanoparticles, or how to regulate them, nearly everyone agrees on the urgency of quickly tackling both questions.

The use of nanoparticles in consumer products like cosmetics and cleaners represents only a tiny sliver of nanotech's potential, but any unresolved safety concerns could cast a huge shadow. "If I was someone producing these materials, I would be afraid that one health problem, anywhere, would hurt the entire industry," says Peter Hoet, a toxicologist at the Catholic University of Leuven, in Belgium.

The large consumer corporations DuPont and Procter and Gamble participated in a study on nanoparticles' toxicity. But the nanotech community needs to put pressure on manufacturers using the "nano" label for marketing purposes to stand up and take responsibility for their products. That means contributing resources and money to toxicity studies and freely disclosing which nanotechnologies they are relying on. TR

Philip E. Ross writes on science and technology from New York City.

Reviews

Books, artifacts, reports, products, objects

MEDICINE

Drug Trials and Error

Conspiracy theories about big pharma would amuse, if they were not a matter of life and death. **By Amanda Schaffer**

In March, *Harper's* magazine, ordinarily classy, bohemian, and reliably well written and reported, went ape. The venerable journal published an account of clinical drug trials that was more baleful (and more fantastic) than that painted by John le Carré in his 2000 novel *The Constant Gardener*, where pharmaceutical companies and governments murderously collude to hide the truth about an experimental drug.

"OUT OF CONTROL"
By Celia Farber
Harper's, March 2006

"A NATION OF GUINEA PIGS"
By Jennifer Kahn
Wired, March 2006

The *Harper's* story, "Out of Control," by Celia Farber, is an extraordinary, overheated document. Farber is a polemicist, notorious for advancing the "Duesberg hypothesis": the argument, proposed by University of California, Berkeley, virologist Peter Duesberg, that HIV does not cause AIDS. Instead, as Farber writes in *Harper's*, "It could very well be the case that HIV is a harmless passenger virus that infects a small percentage of the population and is spread primarily from mother to child." Like Duesberg, Farber believes that in the United States and Europe, AIDS sufferers have poisoned themselves: "many cases of AIDS are the consequence of heavy drug use, both recreational (poppers, cocaine, methamphetamines, etc.) and medical (AZT, etc.)." In Africa, she argues, AIDS is a kind of confidence game played by pharmaceutical companies and national governments: she uncritically offers up Duesberg's position that "AIDS in Africa is best understood as an umbrella term for a number of old diseases, formerly known by other names, that...do not command high rates of international aid." Duesberg (and, we presume, Farber) consequently believes that *all* anti-HIV medications are poisonous shams promoted by self-serving researchers, executives, and activists: "If toxic AIDS therapies were discontinued, [Duesberg] says, thousands of lives could be saved virtually overnight."

Of course, the epidemiological evidence does not support the Duesberg hypothesis. Most virologists, and nearly all AIDS researchers, accept that HIV causes AIDS. Farber's own views of HIV and AIDS drugs seem political, informed by an idiosyncratic set of dislikes: of AIDS activists, of big business, of pharmaceutical and recreational drugs, and of something called "the scientific-medical complex."

Farber's assault on what she calls "the HIV theory of AIDS" is not new: she has been writing approvingly of Duesberg since the late 1980s. What is novel in "Out of Control" is her criticism of an HIV drug trial, called HIVNET 012, that took place in Kampala, Uganda, in the late 1990s. Just *how* drug trials in the poor world should be managed is a real question, and a highly topical one. The same month that *Harper's* unleashed Farber, *Wired* magazine published "A Nation of Guinea Pigs," a story by Jennifer Kahn that addresses the outsourcing of drug trials to India. Portrayals of corrupt or dubious medical research have suddenly become a media genre, one that draws upon popular distrust of the motives and methods of pharmaceutical companies (a psychology that science writer Jon Cohen has dubbed "pharmanoia").

HIVNET 012, funded by the National Institutes of Health, found that a brief, inexpensive regimen of a drug called nevirapine—one shot for a mother at the beginning of labor and one for her infant shortly after birth—could dramatically reduce rates of mother-to-child transmission of the virus. But problems with HIVNET 012 have since come to light: audits and reviews have found that record keeping was sloppy, and adverse events were underreported by trial investigators. Farber believes that these failures suggest a conspiracy to promote drugs that are toxic.

To further discredit HIVNET 012 and support her argument that anti-HIV drugs are deadly, Farber also tells the story of Joyce Ann Hafford, an HIV-positive, pregnant mother in Tennessee, who in 2003 entered another drug trial called PACTG 1022, designed to test anti-HIV drugs on pregnant women. While taking nevirapine in combination with other drugs, and for a longer

MICHEL DE GROOT/WPN

time than the HIVNET 012 subjects did, Hafford developed terrible symptoms, including rashes, nausea, pain, and breathing trouble. She died soon after giving birth, probably from drug toxicity. Farber asserts that the trial was unethical, that nevirapine is unacceptably dangerous and useless, and that Hafford "never had AIDS, or anything even on the diagnostic scale of AIDS." She implies that Hafford was probably not even HIV positive.

The clinical trial in which Joyce Ann Hafford enrolled *did* find nevirapine to have greater-than-expected toxicity when used in combination with other drugs in a particular regimen. These results were reported and published and led to a revision in Federal Drug Administration guidelines for the drug's use. Hafford's death, in which nevirapine was almost certainly a contributing cause, was a tragedy. It does not follow, however, that the risks of nevirapine will always outweigh the benefits, or that the drug is never a good treatment. HIV is a potentially fatal virus, and some of the treatments capable of holding it in check have dangerous side effects (as is also true of some anticancer regimens, such as chemotherapy). It should also be noted that Farber's claim that Hafford did not have AIDS or was not HIV positive is not substantiated.

Farber's treatment of HIVNET 012 is equally cavalier. She writes, "Although HIVNET was designed to be a randomized, placebo-controlled, double-blind, Phase III trial of 1,500 mother/infant pairs, it wound up being a no-placebo, neither double- nor even single-blind Phase II trial of 626 mother/infant pairs." She implies that this degradation in standards occurred because the Ugandans were corrupted by "the lucrative promise of AIDS drug research" and is scandalized that the results of the study were "received rapturously." She concludes, "With the results of the study now published in *The Lancet*, Boehringer [a German pharmaceutical company]...pressed for FDA approval to have nevirapine licensed for use in preventing the transmission of HIV in pregnancy."

By implication, therefore, HIVNET led to the death of Joyce Ann Hafford.

Most of these claims are false or misleading. HIVNET 012 *was*, in fact, a randomized, single-blind phase III trial—that is, a trial primarily designed to study the efficacy of a new drug (in this case, nevirapine), where patients randomly receive either the new drug or the standard treatment for a disease (here, AZT). It was not double blind, because the drug administration procedures were different in the two arms of the trial; but while phase III trials are, ideally, double blind, the FDA does not absolutely require them to be. Similarly, placebos, while desirable, are not strictly necessary to yield scientifically valid trial results. In the case of HIVNET 012, hospital clinicians resisted giving patients placebos, allowing AZT to stand in their place

for purposes of control: they wanted to provide treatments to sick people.

But HIVNET 012 was certainly flawed; NIH itself acknowledges as much. In 2004, the agency therefore requested an evaluation of the trial results from the Institute of Medicine (IOM), an independent, quasi-academic body that advises government agencies and researchers. The IOM concluded that HIVNET 012's conclusions were valid. It agreed that investigators' files had been messy (in part because the hospital in Kampala flooded during the investigation) and that some adverse events had gone unreported (both in patients taking nevirapine and in those taking AZT). But the IOM determined that the data on rates of HIV infection and survival did indicate the benefit of the nevirapine regimen to the newborns.

Ultimately, Farber's contentions are skewed by her assumptions. To someone who believes HIV is benign, what could possibly be a *good* anti-HIV drug or trial?

In any case, HIVNET 012's flaws are not relevant. At least five other studies have now confirmed the safety and benefits of the drug. Indeed, as a group of renowned AIDS experts, including Robert Gallo, the codiscoverer of the HIV virus, wrote recently in response to Farber's article, "Not a single life-threatening event related to short-course nevirapine has been recorded in mother or child in tens of thousands of such uses around the world." Ultimately, Farber's contentions are skewed by her assumptions. To someone who believes HIV is benign, what would be a *good* anti-HIV drug or trial?

Jennifer Kahn's *Wired* story poses different and less easily answered questions about clinical trials in the poor world. Her account of drug trials in India indulges in its own kind of excess: she claims that "India, the brilliant hub of outsourced labor, was positioning itself in a newly lucrative role: guinea pig to the world." But Kahn's piece is genuinely thought-provoking. It profiles a quiet doctor named S. P. Kalantri who works in Sevagram, a town in the middle of India, in order to ask whether clinical trials in the poor world are inescapably morally compromised.

Kalantri explains that he and his hospital are receiving a growing number of requests from pharmaceutical companies looking for test sites for drugs in their development pipelines. On the one hand, he notes, impoverished patients enrolling in these trials can receive a "health care windfall," including regular physical exams and access to medication that may help them. But the problem, Kalantri says, is that patients are often quite passive and tend not to question their doctors' recommendations, making it harder to ensure uncoerced, informed consent. And regrettably, the drugs being tested in India often have little relevance to their recipients' most pressing medical problems. For instance, Kalantri's hospital is currently part of a trial to determine whether a drug called Aggrenox can help to forestall second strokes. Arguably, many other potential therapies would be more helpful to the people of Sevagram. And even those that are helpful may turn out to be too expensive for them.

In "A Nation of Guinea Pigs," Kahn worries that payments to hospitals and doctors, which are meant to cover the costs of running and overseeing a trial, sometimes serve as bribes, encouraging improper human experimentation. She questions whether trials in remote areas receive proper oversight, from either the Indian government or foreign institutions. (Indeed, pharmaceutical trials that do not receive government funding are overseen by commercial institutional review boards, which are paid by the companies they are supposed to be monitoring—an obvious conflict of interest.) Kahn does not demonstrate specific wrongdoing or scandal. But she clearly explains the perverse incentives that *might* encourage unethical behavior.

There are, however, very strong medical, scientific, and economic arguments for conducting clinical trials in the poor world. The drugs tested might be intended for the population testing them; the trials might benefit from genetic diversity; or the trials, usually the most expensive part of the drug development process, might be cheaper. Given that clinical trials *will* be conducted in the poor world, what would be a better system?

The ethical requirements for human research were established by international agreements such as the 1964 Helsinki declaration. They include various commonsense rules: for instance, physicians ought to consider the health and well-being of subjects above other considerations; any adverse effects that occur during the course of a study should be scrupulously monitored, reported, and treated; researchers must fully communicate potential risks and benefits; and subjects must not be coerced into participating. Most importantly, the subjects of a trial should benefit personally from the results of the research (that is, they should not be induced to participate in a trial for solely economic reasons).

But obvious difficulties arise in interpreting these principles and applying them in impoverished settings. A common dilemma is, Just what constitutes excessive inducement? If researchers pay for their subjects' transportation and lunch, or reimburse them for missing a day of work, is that a bribe? What if they offer direct payments?

Informed consent is particularly elusive in places where patients are not well educated and where doctors' authority looms large. Informed-consent agreements are lengthy, bureaucratic documents. One recent improvement is

You spend 1/3 of your life in bed.

Isn't it worth investing in the perfect mattress?

Why is it that we spend more time researching a car we're going to drive a few hours a week than we do a bed where we spend a third of our lives? Especially when the amount and quality of our sleep directly impacts our physical and mental health.

Tempur-Pedic's Weightless Sleep™ Technology delivers unparalleled comfort.

ONLY FROM TEMPUR-PEDIC®
AUTHENTIC™
TEMPUR® Material

Each Tempur-Pedic Swedish Mattress™ contains billions of viscoelastic cells that gently settle to support every contour of your body. The mattress molds itself to your body shape, taking pressure off of your neck, back, shoulders and hips. You'll feel like you're sleeping on a cloud because every part of your body receives complete and relaxing support. Recent research even indicates that Tempur-Pedic beds reduce nighttime tossing and turning by more than 70%.

Make the right investment for better sleep and health.

You deserve a mattress that's going to help you sleep soundly and wake up refreshed every morning.

Others Agree:

Ease-of-Use Commendation By ARTHRITIS FOUNDATION www.arthritis.org

CONSUMERS BEST BUY DIGEST

SPACE

THE *ONLY* MATTRESS RECOGNIZED BY NASA AND CERTIFIED BY THE SPACE FOUNDATION ✦

LIMITED WARRANTY TO CONSUMERS
Good Housekeeping Promises
REPLACEMENT OR REFUND IF DEFECTIVE

Call 888-225-8021

today for your FREE Tempur-Pedic Demo Kit!
It's a toll-free call.

TEMPUR-PEDIC®
PRESSURE RELIEVING
SWEDISH MATTRESSES AND PILLOWS

Changing the way the world sleeps!®

to supplement documents with visual aids and require patients to answer a brief quiz to ensure they have really comprehended the nature and terms of the transaction. It is important that patients understand they may leave the trial whenever they wish and will neither be punished nor lose their primary health care.

Among the most vexing questions is, Who should oversee the people who oversee clinical trials? At NIH, where HIVNET 012 has cast a long shadow, there is a growing interest in supporting the work of local ethics committees. But local groups often lack the training and resources to do much. One study, which appears in the March-April issue of *IRB: Ethics and Human Research*, suggests that many African groups are susceptible to influence and have limited expertise.

A variety of promising initiatives, sponsored by international bodies like the World Health Organization (WHO), may help these groups to grow stronger. WHO is funding projects that teach ethics and provide infrastructure. This sounds sane: American and European private and public institutions cannot provide the oversight required for ethical clinical trials in the poor world, particularly when American and European pharmaceutical companies are involved.

Read together, the Farber and Kahn pieces, apparently so different, disturb. While Farber's malignant vision of clinical trials is obviously unhinged, it does remind us that clinical trials are not without risks for their subjects. Kahn dramatizes another uncomfortable fact: that economic disparity between investigators and subjects in human research creates possibilities for abuse and coercion—possibilities that we do not really know how to manage. Considered in combination, these realities may not justify pharmanoia, but they explain it. TR

Amanda Schaffer writes about science and medicine for Slate.

SILICON VALLEY

Who's Sorry Now?

Pip Coburn was a star research analyst during the Internet boom. Today, he thinks the entire technology industry has to change.

By Jason Pontin

Time was, I thought about this stuff all the time. I mean Silicon Valley and the venture capitalists who invested in its startups, and the financial analysts who promoted the companies its investment banks took public. I thought about it because from 1996 to 2002 I was the editor of *Red Herring* magazine, sometimes called the "bible of the boom." It was an entire world, one that today seems to me as antediluvian as Noah's seaside villa.

I thought about Pip Coburn pretty often, too, because he was the managing director of the technology group of UBS Investment Research, an investment bank, in charge of its 120 technology and telecommunications analysts, and thus a considerable man in the New Economy. But I also thought about him because he wrote a column for *Red Herring* from late 1999 until shortly before the magazine's collapse in 2003. (The magazine has since been relaunched, in more modest form.)

THE CHANGE FUNCTION: WHY SOME TECHNOLOGIES TAKE OFF AND OTHERS CRASH AND BURN
By Pip Coburn
Portfolio, 2006, $24.95

The cover of the May 2000 issue of *Red Herring* blazes, "Who Wants to Be a Billionaire?" Flipping through its 480 pages of executive profiles, corporate analysis, econometric data, and an endless succession of "tombstones," (where investment banks advertised successfully managed initial public offerings), I can still find Pip's column, called "Tactics." There I read, "What characterizes a practical framework for tech investing? First, accept life in the tech fishbowl the way it is…as opposed to the way it should be, which is rational." That was almost certainly written in February, *one month* before the Internet bubble burst.

Arguably, Pip Coburn has a great deal to explain, although not as much as some analysts of that era: in *Red Herring*, and in his research reports, he was reliably skeptical about earnings growth estimates for technology companies, and he never hawked stocks he secretly despised. But as he writes in his first book, *The Change Function*, "I wasn't spending too much time at *that* time thinking about the elephant head on the table [he means the overvaluation of technology stocks]…because it really was a lot of fun participating in Nasdaq's run from 333 on October 10, 1990, to the 5,008 peak on March 10, 2000."

Coburn would have reason to repent of his high spirits: by 2002, the Nasdaq stock exchange had lost 80 percent of the value it had at its height. As I write, Nasdaq is at 2,368, and the technology industry has never recovered the ebullience it enjoyed in the 1990s. *The Change Function* therefore represents a settling of accounts, although its author would deny it. Coburn (who now works for Coburn Ventures, a consultancy that he founded, dedicated to putting "its knowledge about 'change' to work in the realm of technology, telecom, and media investing," according to the company's website) writes, "The purpose of this book is really quite simple. I think there's a problem, and I'm proposing a solution.…The technology industry has become self-absorbed as a result of five decades of success.…Over time, technologists have become increasingly focused on creating miracles, even if it's rare that those miracles translate into commercial success."

The attractively simple thesis of *The Change Function* is that most technology ventures fail because technologists manage them. Technologists think their business is the creation of cool technologies loaded with wonderful new features. They think this because they are engineers who thrill to the idea of change. By contrast, Coburn says, "technology is widely hated by its users," because ordinary folk loathe change. Therefore, any new artifact, no matter how much its various features might appeal to technologists, will *always* be rejected by its intended customers unless "the pain in moving to a new technology is lower than the pain of staying in the status quo."

Or in Pip's geeky formulation:

The Change Function = f (perceived crisis vs. total perceived pain of adoption).

This makes goofy sense of why technologies succeed. At any rate, it reflects how *I* adopt new technologies: unwillingly, and because I must. But the change function really takes off as an explanation of why technologies fail.

Coburn calls companies run by technologists "supplier oriented." The crisis technologists are solving is their own: they want to justify the expectations of investors and their own hopes for influence. But they do not understand the change function. Technologists think a new technology is adopted when it is ten times better than anything else (former Intel CEO Andy Grove's law of 10x disruptive technologies), and at the same time, the price of the technology drops because the complexity of an integrated circuit, relative to its minimum component cost, doubles every two years (Intel cofounder Gordon Moore's Law).

Or according to Pip:

Supplier-centric adoption model = f (Grove's law of 10x disruptive technology × Moore's Law).

The supplier-centric adoption model is dangerously limited, according to Coburn. Users want incremental improvements to technologies they already possess. Price is only a secondary influence. Coolness is not a necessary input to the change function, unless feeling uncool precipitates a crisis of identity. Thus, Coburn says, because almost all technology ventures are supplier oriented, "90 percent of VC bets fail."

Put another way, as Jean-Louis Gassée, the founder of Be Inc., once told me, "The most expensive idea in Silicon Valley is, 'It will work, because it would be really cool if it did.'"

ERIC HANSON

Coburn's solution is that technology companies, and the technologists who work for them, must suppress their inner geek and become "user centered" and "[figure] out what people want." To discover what people really want (something Pip concedes we hardly know of ourselves), he proposes that technologists employ "sociologists, anthropologists, communication consultants, change consultants, professional observers, futurists, and folks who just study change a whole heck of a lot." This last may be read as a muted plea to employ Coburn Ventures.

All this is amusing and stimulating, but is it *true*? As someone who saw firsthand the ruin that Coburn describes, I can definitively say, *kind of*. Having removed the distorting lenses of financial euphoria, we can see that technology companies fail unacceptably often. Also, most new technologies have too many features that no one wants. Finally, the notion of the change function itself is persuasive: an elegant property of Coburn's big idea is that it accounts for change of *all* kinds, including personal reformations like dieting or kicking drugs. But Pip's insistence that users hate change and only want incremental improvements to existing technologies seems an excessive reaction to the recent past: sometimes new technologies really are, in Apple CEO Steve Jobs's famous phrase, "insanely great." To use Coburn's own language, people who saw the first Macintosh computer or Web browser experienced crises of covetousness.

Will *The Change Function* achieve the author's stated purpose of reforming an industry that is *still* supplier-centric? It need not convince anyone. Eventually, Coburn says, the industry's crisis in confidence will outweigh the pain it feels in abandoning the gratifying illusion that cool technology and falling prices are sufficient to command users' loyalty.

Such change couldn't come too soon for Pip. In a recent conversation, he explained to me why he wrote his book: "One day, I thought of all the companies who had come to see me, and I felt some resentment. They really only served themselves. I realized it's not about the supply [of technology]—there'll always be supply—but about what causes *real* change." Which is as close to an apology as we are likely to get from someone so complicit in inflating the last bubble. TR

Jason Pontin is Technology Review*'s editor in chief.*

NATIONAL DEFENSE

The Great Transformation

Why are the champions of Reagan's defense buildup arguing for a smaller, more technological military? **By Mark Williams**

John Arquilla himself might describe his new book on foreign policy as an academic text, unlikely to be noticed or discussed beyond a small circle of professors and policymakers. But he has insight into American national strategy and knows a lot about new military technologies, and a few of his passing claims in *The Reagan Imprint* might make it grist for future historians.

One such claim is that one man, Andrew Marshall, was primarily responsible for proposing to Ronald Reagan in the early 1980s that the United States ratchet up its military spending, in order to prompt an arms race that would be so economically punishing it would help dispatch the Soviet Union to the dustbin of history.

THE REAGAN IMPRINT: IDEAS IN AMERICAN FOREIGN POLICY FROM THE COLLAPSE OF COMMUNISM TO THE WAR ON TERROR
By John Arquilla
Ivan R. Dee, 2006, $26.00

It's a plausible assertion. If one speculated about the identities of the specific architects of Reagan's strategy, it would be hard to think of a *more* likely candidate than Marshall, who through seven presidencies, and now in his mid-80s, has remained the reclusive, semilegendary director of the Office of Net Assessment, the Pentagon's in-house think tank of strategic analysts and futurists. Certainly, John Arquilla—a consultant to Santa Monica, CA–based think tank Rand, Pentagon advisor, and professor at the Naval Postgraduate School in Monterey, CA—has an insider's knowledge. He also has an agenda, however.

In *The Reagan Imprint*, Arquilla writes that his book's raison d'être was his "deepening sense of unease about the general direction of American foreign policy and national security strategy.…The United States is squandering the remarkable reversal of fortune in world affairs that Ronald Reagan engineered." By reassessing Reagan's strategic legacy, Arquilla proposes, we might understand how American policy needs to be adjusted.

As the titles of his previous books suggest—*Networks and Netwars: The Future of Terror, Crime, and Militancy*, or *In Athena's Camp: Preparing for Conflict in the Information Age*—Arquilla is among a corps of defense thinkers who, following Marshall's lead, have promoted the concept of U.S. military "transformation." Nowadays, transformation, in its specialized sense, is an official policy of the U.S. military, instituted by another Marshall acolyte, former Rand chairman Donald Rumsfeld. "Transformation" was considered an easier word for the Pentagon's generals and admirals to swallow than "revolution"—as in "revolution in military affairs," or RMA, which was how Marshall and the other originators of the concept first described their big idea.

As either transformation or revolution, however, the policy entails moving America's armed services away from the massed forces and big weapons systems of the 20th century and toward smaller organizational units that use modern information, communications, and robotics technology to mount the kind of agile campaign seen in Afghanistan in 2001.

Long-range smart missiles, drone aircraft, and cyber attacks on enemies' communications systems are all part of the vision of transformation. Longer-term plans call for even more advanced technologies. The massively ambitious Future Combat Systems program, for instance, will create a "system of systems" networking all elements of the U.S. armed services to enable unprecedented levels of joint connectivity and "battlespace" awareness. Bolder still is the Future Warrior Concept effort, which the U.S. Army is conducting in tandem with MIT: by 2020, it will supposedly have produced the ultimate infantryman's kit, integrating fluid-based body armor that hardens in a thousandth of a second and a nanotechnology-based powered exoskeleton. Researchers are unabashed to admit that the battle suits in *Starship Troopers*, Robert Heinlein's classic science fiction novel, were an inspiration.

Expensive new toys are, of course, usually welcomed at the Pentagon. But in the vision laid out by Andrew Marshall and his followers, transforming the U.S. military will ultimately mean fewer generals and admirals with fewer big toys—fewer aircraft carrier battle groups, fewer heavy-tank divisions, and fewer next-generation fighter planes. So while the American military establishment pays lip service to transformation, its actual attitude has been along the lines of St. Augustine's prayer: "O Lord, help me to be pure, but not yet."

The Reagan Imprint is best understood as, partly, Arquilla's attempt to sell transformation in its pure version. A smaller, more agile military would be cheaper, better suited for today's regional conflicts, and less antagonizing to other nations, he argues.

Arquilla maintains that even Reagan's massive conventional military buildup should be understood in terms of his desire to prevent any future conflict between NATO and Warsaw Pact forces from escalating into a thermonuclear exchange. Because NATO war games in Europe during the 1970s had regularly ended with the American commander calling for use of tactical nuclear weapons to fend off numerically superior Soviet conventional forces,

JOSEPH SOHM, VISIONS OF AMERICA/CORBIS

Reagan asked the Pentagon what was necessary to avoid that contingency. The military responded, predictably, that it would need tens of billions more dollars for more troops and technology. Reagan was willing to foot the bill, and—according to Arquilla—the ensuing buildup also served to implement Marshall's 1981 proposal that US. military funding be increased to a level that would be punishingly difficult for the U.S.S.R. to match.

The strategy worked. But as a result, Arquilla insists, the Pentagon learned to regard massive defense budgets as its due. The Center for Arms Control and Non-Proliferation estimates that the U.S. military will spend more than $550 billion in fiscal year 2007, plus an additional $50 billion Pentagon request to support operations in Iraq and Afghanistan. That's a larger budget than many from the Cold War years and more than the *combined* military spending of every other country in the world.

Unfortunately, Arquilla argues, the U.S. military's beloved "big platform" systems have few practical applications against the enemy America now faces: a global terrorist insurgency. The transformation programs pushed by Marshall, Rumsfeld, Arquilla, and others are proceeding: investments in special forces, drone aircraft, and the like will increase by 15 percent in 2007, and networked, downsized, and nimble units have been assembled. But the Pentagon remains generally disposed to military gigantism. Most of the $84 billion in weapons spending called for in the Department of Defense budget is being misdirected, Arquilla believes, to items like the F-22 and F-35 fighters, advanced warships for surface combat and coastal warfare, and the CVN-21, the navy's next-generation supercarrier, which will start construction in 2007 and be bigger than today's Nimitz-class carriers—already the largest warships ever built.

In addition, Arquilla says, maintaining a mass army to deal with other old-style mass armies will increasingly and needlessly put hundreds of thousands of American servicemen and women in harm's way, as smart, precision-targeted weapons like cruise missiles become progressively cheaper and more accessible to other governments or groups.

Even a war against an increasingly militaristic China would not necessarily involve armies of millions or fleets of expensive warships, Arquilla argues; the Chinese themselves, rather than building aircraft carrier battle groups, are developing technologies like maneuverable sea-going mines, supersonic antiship missiles, and supercavitation torpedoes, which move at hundreds of knots by pushing a friction-reducing bubble of air before them. In a world of ever more-accurate weapons, the Pentagon's continuing allegiance to its giant platforms and systems is increasingly likely to be the downfall of U.S. forces in battle, Arquilla insists.

Some of the surgical military measures Arquilla advocates would offend conventional wisdom. In *The Reagan Imprint*, he laments that Reagan's secretary of defense, Caspar Weinberger, blocked the initiation of a "war on terror" that the president had approved in a still-classified 1984 document, National Security Decision Directive No. 138. The directive apparently authorized secret CIA and FBI paramilitary squads, alongside military units like the navy's SEALs and the army's special forces, to undertake preëmptive and retaliatory sabotage and targeted killings.

Unlovely as some of this may seem, Arquilla's strategic stance has several virtues. First, it's preferable to the traditional Pentagon methods to which the U.S. may resort in the case of a "long war" against Islamic fundamentalists. Second, whether or not defense gigantism is a recipe for military disaster, today's level of spending on big-platform systems is simply economically unsustainable: government budgets are about to feel enormous new pressures as baby boomers retire and Medicare, Medicaid, and Social Security spending balloons. Third, Arquilla's propositions offer a route to reducing the American military's visibility around the world.

In a world where technology is placing ever greater destructive power in the hands of ever smaller groups, the possibility of megaterrorism has emerged. In such a world, John Arquilla is unashamed to point out, keeping a lower profile might be a sensible U.S. military strategy. TR

Mark Williams is a contributing writer at Technology Review.

Nanocrystal Displays

QD Vision's Seth Coe-Sullivan is using quantum dots to make vibrant, flexible screens. **By Kevin Bullis**

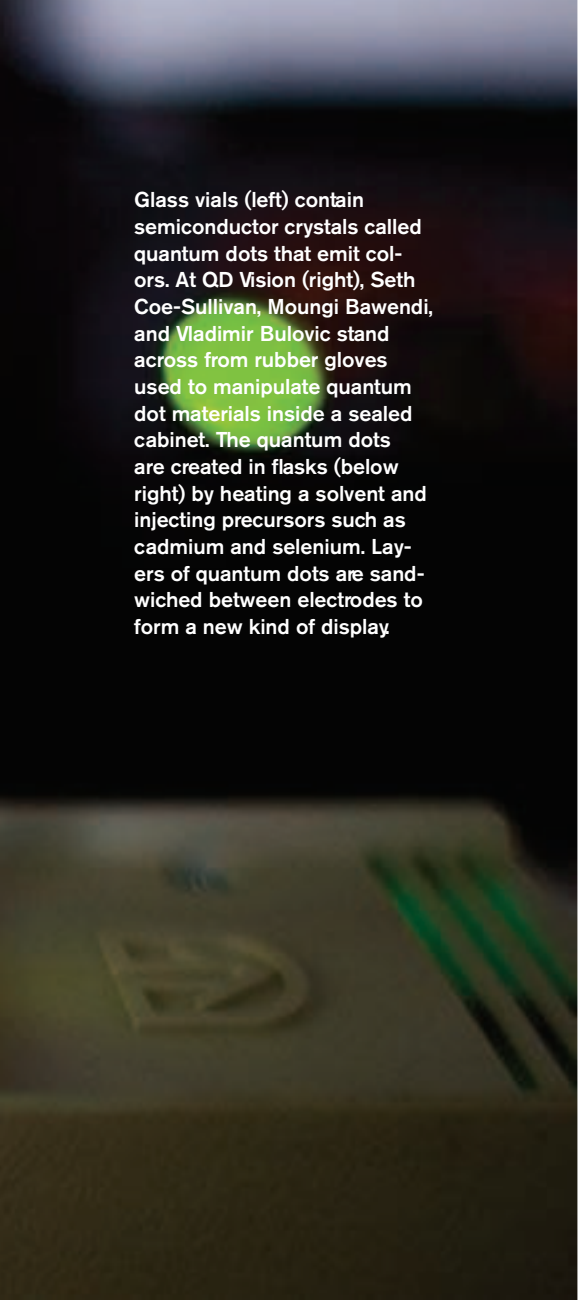
Seth Coe-Sullivan, chief technology officer at Watertown, MA, startup QD Vision, fastens alligator clips to two edges of a transparent wafer the size of a cell-phone screen and flips a switch: a rectangle filling the center of the wafer suddenly turns from reflective silver to faint red. A lab worker turns off the room lights to heighten the effect—but this isn't necessary. Coe-Sullivan turns a knob and the device begins glowing brilliantly.

This is QD Vision's first display—a monochromatic 32-by-64-pixel test bed for a technology Coe-Sullivan hopes will replace those used in today's high-definition TVs. Thin and flexible, the next-generation display will be easy to see in sunlight and less power hungry than the one in your current laptop, he says. It will also cover more of the visible color spectrum than current displays and produce such high-contrast images that today's flat-screen displays will look dull and washed out by comparison.

At its heart are nanoparticles called quantum dots, nanoscale semiconductor crystals. By altering the size of the particles, researchers can change the color they emit: for example, a six-nanometer-diameter particle would glow red, while another of the same material but only two nanometers wide would glow blue.

Where these particles really shine is in the purity of the colors they emit. Displays create millions of colors from a palette of just three: each pixel is made of a red, a green, and a blue subpixel, and varying their relative intensities varies the pixel's apparent color. In LCDs and organic light-emitting devices (OLEDs), a new kind of display, the subpixel colors are impure. The red, for example, while made mostly of red light, also contains smaller amounts of other colors. With quantum dots, however, the red subpixel emits only red.

This purity means quantum dot–based displays have more-saturated color than LCDs, OLEDs, and even bulky cathode-ray tubes (CRTs), which are still prized for their excellent color rendition. What's more, Coe-Sullivan



Glass vials (left) contain semiconductor crystals called quantum dots that emit colors. At QD Vision (right), Seth Coe-Sullivan, Moungi Bawendi, and Vladimir Bulovic stand across from rubber gloves used to manipulate quantum dot materials inside a sealed cabinet. The quantum dots are created in flasks (below right) by heating a solvent and injecting precursors such as cadmium and selenium. Layers of quantum dots are sandwiched between electrodes to form a new kind of display.

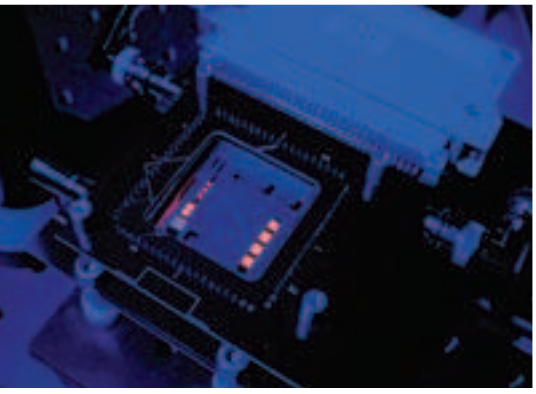
says, the range of colors possible in a quantum dot display is 30 percent greater than in CRTs: "We're increasing the depth of the green that screens can display, and the depth of the blue-green, et cetera. It's actually a different color than can be seen on an LCD, OLED, or CRT."

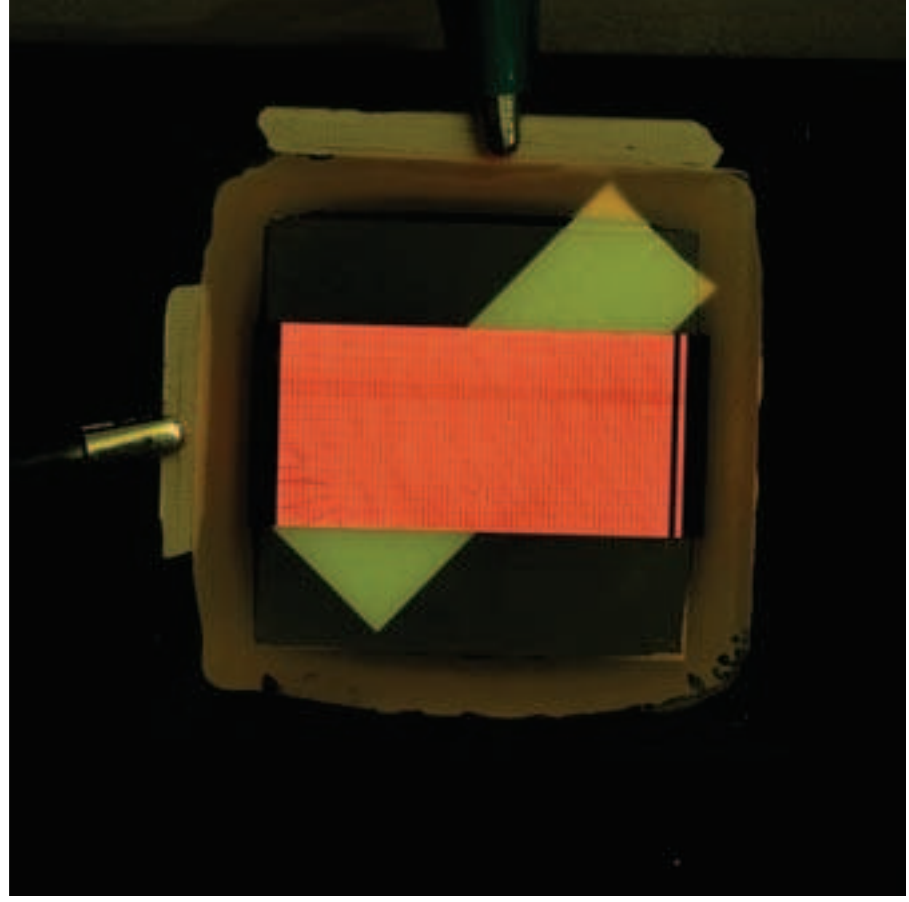
Perhaps what is most exciting about quantum dot LEDs (QD-LEDs) is that they use much less power than LCDs. In LCDs, a backlight illuminates every pixel on the screen. Dark pixels are simply blocking this light, in effect wasting energy. In part because quantum dots emit light rather than filtering it, a QD-LED display could potentially use one-30th the power of an LCD.

And there's another benefit to not having a backlight, according to Vladimir Bulovic, an expert at MIT in OLED displays. Because in LCDs the dark pixels don't block light perfectly, Bulovic says, the "black" pixels on LCDs are really just dark grey. With quantum dots, on the other hand, black pixels emit no light. "What makes the picture crisp and really jump out at you is that the black is really, really dark," he says.

"Beakers of This Glowing Green Stuff"

The idea to use quantum dots in displays is not new. In the early 1990s, when chemists such as Moungi Bawendi, now an MIT professor of chemistry and scientific advisor at QD Vision, were perfecting techniques for forming precise, uniform quantum dots, some tried to make QD-LEDs but produced only dim, inefficient devices that required about a hundred





Coe-Sullivan (top left) holds a prototype quantum dot display; such displays emit extremely pure colors and could eventually be scaled up to compete with conventional screens. When plugged in (above), the display reveals its pixels, which in this case form a red rectangle on the screen. QD Vision scientists continue to improve the devices (bottom left), testing color, brightness, and efficiency.

thousand electrons to coax quantum dots to emit a single photon. In contrast, Coe-Sullivan's QD-LEDs require only about 50 electrons per photon.

Achieving this advance required the right people to come together at the right time. That happened in 2000, when Coe-Sullivan came to MIT as a graduate student and met Bawendi and a brand new MIT electrical-engineering professor who had arrived a few weeks before—Vladimir Bulovic.

Just inside the door to QD Vision's lab is a row of flasks containing a bubbling red liquid—a solution of recently formed quantum dots. The collaboration that led to the first efficient QD-LED display began after Bulovic, on a visit to MIT, stumbled upon a similar scene in the lab of one of Bawendi's collaborators.

Bulovic says that before he encountered "beakers of this glowing green stuff" at MIT, he had "never heard of quantum dots." Coe-Sullivan borrowed Bulovic's knowledge of OLED fabrication tricks and Bawendi's quantum dot expertise and also enlisted the help of fellow students Jonathan Steckel and Wing-Keung Woo.

Even with all this expertise, however, the breakthrough that enabled the device occurred partly by accident. The researchers had mixed quantum dots into a solution of organic molecules and spread the mixture into a thin film using a process called spin-casting, in the hope that the quantum dots would disperse evenly through the film. As it turned out, the quantum dots rose to the surface of the film and assembled in an orderly, uniform layer just one dot thick, an arrangement that turned out to be more efficient than the one the researchers had intended.

This layer of quantum dots became the core of a multilayer single-color QD-LED, sandwiched between electrodes and charge transport layers. Coe-Sullivan, along with Bulovic and Greg Moeller, director of business development, founded QD Vision in 2004 to move from this simple device to a full-color display that can be profitably manufactured.

A major step was arranging arrays of pixels. At QD Vision, Coe-Sullivan points to a glass-front cabinet carefully blocked off to hide part of a proprietary process for distributing quantum dots in the alternating three-color rectangular grids necessary for a working display. Already the technique, which Coe-Sullivan says should lead to relatively inexpensive manufacturing, has produced patterns with pixels smaller than those typical of current displays.

Coe-Sullivan says QD Vision should be able to borrow from OLED technology one key component of displays, the "back plane" that controls the pixels. Now the company is focused on improving the efficiency of its device, which, while competitive with cell-phone displays, could still be improved.

In all, Coe-Sullivan says he expects that it will be about four years before the company has its first commercial product—probably a small display for a cell phone. But he says the colorful images will be worth the wait. TR

HEALTHY CELLS. HEALTHY AGING.

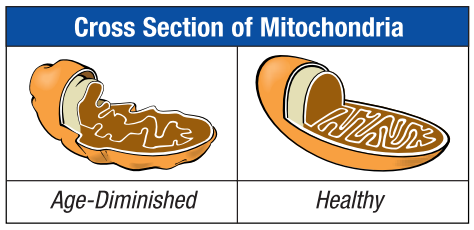
The Science of Aging.

FOR YEARS, SCIENTISTS HAVE BEEN INVESTIGATING THE SECRETS OF AGING. Dr. Bruce Ames, a renowned geneticist, leading biochemist and University Professor, has studied the relationship between diet, maintaining healthy cells, and the aging process. His research focuses on the links between aging and tiny structures inside cells called mitochondria.

Mitochondria are the powerhouses of our cells, the biological engines that convert carbohydrates, fats and proteins into the energy used by the entire body. Aging mitochondria are less efficient at converting fuel to energy, and they produce more toxic oxidants.

Healthy mitochondria keep our cells healthy. Healthy cells provide energy to support the brain, skin, muscles and cardiovascular system.

Together Dr. Ames and an award-winning team of UC Berkeley scientists discovered in pre-clinical tests, that by using the right combination of a natural, energy-boosting component (acetyl L-carnitine) and a powerful antioxidant (alpha lipoic acid) they could improve the health of mitochondria, thereby slowing the cell aging process. The result is Juvenon™, a cellular health supplement patented by the University.



Taken regularly like vitamins, Juvenon™ works on the mitochondria to improve cellular health and maintain it over the years. The result: healthy aging.

Sustains Energy Level
Promotes Brain Cell Function
Powerful Antioxidant

Order Juvenon Today and Save $5

Promotional Code: T606

www.juvenon.com
1-800-JUVENON
(1-800-588-3666)

100% Satisfaction Guarantee!
Not available in stores.

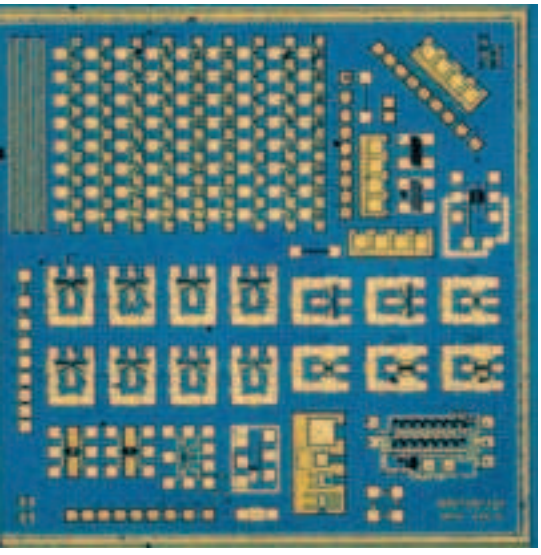
INFORMATION TECHNOLOGY

After Silicon

Microprocessors made of a different semiconductor

SOURCE: "Beyond CMOS: Logic Suitability of $In_{0.7}Ga_{0.3}As$ HEMT"
D. H. Kim and J. A. del Alamo
Paper presented at the International Conference on Compound Semiconductor Manufacturing Technology, April 24–27, 2006, Vancouver, British Columbia

RESULTS: MIT researchers have made a transistor out of a nonsilicon semiconductor that, in early stages of development, provides speed and performance similar to those of state-of-the-art silicon transistors while consuming less power.



A new chip uses indium gallium arsenide.

WHY IT MATTERS: The properties of compound semiconductors such as indium gallium arsenide or indium antimonide make them attractive alternatives to silicon. Electrons move through compound semiconductors as much as 50 times faster than they do through silicon; compound-semiconductor transistors thus operate at a lower voltage, consume less power, and produce less heat that can damage a chip.

The excellent optical properties of compound semiconductors could offer another advantage. Since compound semiconductors easily produce light, photons could potentially zip data between transistors without copper wires.

METHODS: The researchers used a common deposition process to build up layers of indium gallium arsenide and of the insulating material indium aluminum arsenide—the "gate dielectric" that prevents electron leakage between the transistor and its "gate," which turns it on and off. They then used an electron beam to carve out the gate. Finally, the researchers added the metal contacts—made of nickel, germanium, and gold—that are used to put electrons in and take them out of the transistor.

NEXT STEPS: With silicon transistors, the gate dielectric, which is made of an insulator called silicon dioxide, grows on top of the silicon when it is exposed to oxygen. Compound semiconductors, however, have poor interfaces with their oxides. The researchers are conducting tests to determine which gate dielectric material will optimize the performance of their transistors.

Quantum Key Extended

Technique keeps information private over greater distances

SOURCE: "Experimental Quantum Key Distribution with Decoy States"
Yi Zhao et al.
Physical Review Letters 96: 070502

RESULTS: Researchers at the University of Toronto have dramatically increased the distance that a quantum key—photons that represent bits of data for encoding and decoding secret communications—can travel by modifying a commercial quantum encryption system.

WHY IT MATTERS: Quantum encryption is, in theory, a perfectly secure method for communications. Perfect security would require sending an encryption key on the backs of polarized photons, which would be transmitted—either via fiber optics or through the air—one at a time. The peculiar laws of quantum mechanics dictate that, if an eavesdropper picked off just one of these photons, the entire transmission would be altered, prompting the sender to transmit another key along a more secure path.

Unfortunately, no single-photon emitter actually exists. So scientists use the next best thing: strong filters that can winnow a laser pulse down to approximately one photon. Long-distance transmissions, however, require laser pulses of particularly high intensity, which increases the probability that two photons per pulse will slip past the filter. If two identically polarized photons are sent at once, an eavesdropper can pick off one of them without disturbing the other.

Hoi-Kwong Lo and his group used the duplicate photons to their advantage. They purposely generated extra photons that contained no information about the key by passing a laser beam through a *weak* filter instead of a strong one. An eavesdropper wouldn't know which photons held the key and which were decoys.

METHODS: The researchers modified a commercial quantum encryption system by adding a modulator that adjusts the intensity of both decoy and key-carrying laser pulses. The filter allows the person who sends the key to randomly blend both types of pulses into the transmission.

NEXT STEPS: On their first pass, the researchers were able to transmit a blended light signal over 60 kilometers of telecommunication fibers. With some slight modifications, the scientists say, their quantum decoy system will be

COURTESY OF JESUS DE ALAMO/MIT

able to securely send key-carrying photons 120 kilometers, a range comparable to that of commercial systems with less-rigorous security.

NANOTECHNOLOGY

DNA Origami

Simple synthesis could bring nanoscale design to the masses

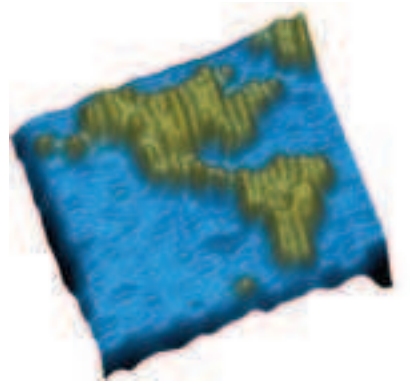
SOURCE: "Folding DNA to Create Nanoscale Shapes and Patterns"
P. W. K. Rothemund
Nature 440(7082): 297–302

RESULTS: Paul Rothemund, a Caltech computer scientist, has developed a simple technique for building nanometer-scale, two-dimensional structures of any shape or pattern from DNA. So far, he's made, among other things, smiley faces, the letters "DNA," and a map of the Western Hemisphere. These structures can also be combined to form larger shapes. Since the shapes "self-assemble" in solution, billions of them can be made at once.

WHY IT MATTERS: DNA is a versatile raw material for nanoscale structures. But past methods of using DNA as a nano building block were slow, labor intensive, and expensive, which limited their use to a handful of labs. The new technique is simple and inexpensive enough for widespread use, Rothemund says. Since a variety of molecules and nanoparticles can be linked to DNA, the technique could be a way of quickly patterning molecules as diverse as proteins and carbon nanotubes, possibly leading to minute electronic devices or "nanoarrays" for studying cells at an unprecedented level of detail.

METHODS: Rothemund begins with a solution containing long strands of DNA with a known sequence. He then adds hundreds of different short "staple strands," each with a sequence designed to latch on to two or three specific sections of the long strand. As the staples connect, they pull these sections together, causing the long strand to fold into the desired shape.

NEXT STEP: Using the technique to make electronics will require the invention of a nanoscale equivalent of the transistor. Also, since any self-assembly process is prone to error, engineers will need to develop fault-tolerant computer architectures. For biological applications, such as sensors that determine the kinds of proteins in a particular cell, researchers will need to find a reliable way to read signals transmitted by the minuscule devices. Rothemund expects that the best applications of the new technique are yet to be imagined.



A 100-nanometer-wide "map" was made with DNA.

PAUL ROTHEMUND/CALTECH

Knitting Nerves Back Together

Nanofibers allow injured brain and spinal tissue to repair itself

SOURCE: "Nano Neuro Knitting: Peptide Nanofiber Scaffold for Brain Repair and Axon Regeneration with Functional Return of Vision"
Rutledge Ellis-Behnke et al.
Proceedings of the National Academy of Sciences 103(13): 5054–5059

RESULTS: Using self-assembling nanomaterials, MIT researchers have restored the sight of brain-damaged rodents. After cutting through a structure in hamsters' brains necessary for vision, neuroscientist Rutledge Ellis-Behnke and colleagues injected the animals with a solution containing short chains of amino acids, called peptides, that when in contact with brain fluids assemble into nanoscale fibers. The resulting mesh of fibers bridges the gap left by the cut and prevents scar tissue from forming, thus allowing neurons to regrow and reëstablish preinjury signal pathways. Seventy-five percent of adult hamsters treated with the technique recovered enough vision to detect and turn toward food.

WHY IT MATTERS: Spinal-cord and brain injuries from accidents, strokes, and disease affect millions of Americans; many of these people never regain lost abilities and functions, largely because scar tissue and inhibitory chemicals prevent damaged tissue from healing. At least over short distances, the experimental nanomaterial seems to overcome these problems in neural tissue. The nanomaterial allows nerve cells to grow and reëstablish connections, which could restore human patients' lost abilities to walk or talk, even as it restored sight in these experiments.

METHODS: In separate experiments on young and adult hamsters, the researchers cut through a brain structure called the optic track, which conveys visual signals, thus blinding the hamsters in one eye. Soon after the cut was made, control animals received an injection of saline at the site of the injury, and test animals received an injection of the peptides. The researchers then tested the animals for the ability to see and turn toward sunflower seeds and, after euthanizing them, examined their brain tissue to measure the regrowth of neurons.

NEXT STEP: If large-animal studies go well, the treatment could be tested in

Executive Education Resource for Technology Leaders

Do you want to broaden your knowledge base? How do you know which executive education or web-based MBA program is right for you? Technology Review's program directory and online resource offers expert tips, articles, and details about top programs to help guide your decision.

To learn more visit: http://www.technologyreview.com/resources/execed/

Program Directory

BABSON MBA

Babson's Fast Track MBA

Babson is the leader in entrepreneurial management education. Babson's Fast Track MBA combines in-person and Web-based learning, to deliver a highly innovative approach to business education. Fast Track also emphasizes team-based learning. You'll learn not only from top educators and business leaders, but also from your fellow students and teammates.

http://www3.babson.edu/MBA/programs/fasttrack/

COLUMBIA BUSINESS SCHOOL

Columbia Business School Programs for Executives

Columbia Business School's degree and nondegree programs combine Ivy League excellence with a street-smart curriculum that leverages our location in the world's business capital. Through hands-on courses that bridge theory and practice, you'll learn how to identify and capture opportunity in today's global marketplace.

http://www.gsb.columbia.edu/emba

HARVARD BUSINESS SCHOOL

Harvard Business School Executive Education

Harvard Business School Executive Education's Leading Product Development program, taking place on campus July 10-14, 2006, offers senior executives cutting-edge leadership and product development tools and methodologies, which will enable them to strategically identify, create, and capitalize on opportunities for continuous innovation. Enroll today by visiting:

http://www.exed.hbs.edu/redirects/lpdtrm/

MITSloan MANAGEMENT

MIT Sloan Executive Education

MIT Sloan Executive Education provides senior executives and managers with the tools and frameworks to drive innovation and turn today's good ideas into tomorrow's successful products and services. From technology strategy to system dynamics, financial engineering to life sciences, we offer cutting-edge programs that reflect the depth and expertise of our faculty and MIT's research distinction.

http://mitsloan.mit.edu/execed/

humans starting within three years. Meanwhile, the researchers are developing ways to speed nerve regrowth, with the goal of reconnecting distant areas of the brain and spinal cord separated by larger injuries.

BIOTECHNOLOGY

Found: A Gene for Diabetes

A common gene variant behind many cases of type 2 diabetes

SOURCE: "Variant of Transcription Factor 7-like 2 (*TCF7L2*) Gene Confers Risk of Type 2 Diabetes"
S. F. Grant et al.
Nature Genetics 38(3): 320–323

RESULTS: Scientists at deCode Genetics in Iceland identified a gene variant that accounts for more than 20 percent of cases of type 2 diabetes. About 30 percent of Americans carry the gene variant; those who have one copy have a 45 percent greater risk of developing type 2 diabetes, while for those who have two copies (about 7 percent of the U.S. population), the risk is 141 percent greater. The gene, called *TCF7L2*, regulates the activity of other genes, and the protein it codes for is involved in a biochemical pathway believed to play a role in the maintenance of proper glucose levels.

WHY IT MATTERS: Scientists have long sought genetic mutations that boost the risk of type 2 diabetes. But the complexity of the disease, which is linked to both environmental and genetic factors, makes the task difficult. The gene identified by deCode is the best genetic predictor of the disease found to date and may point the way to new drug targets.

METHODS: DeCode scientists looked at 228 variable genetic markers on a previously identified region of chromosome 10 among 2,000 diabetes patients and controls in Iceland. They identified one version of one marker that correlated with an increased risk of diabetes. They then confirmed the findings in an American and a Danish population.

NEXT STEPS: DeCode scientists now plan to develop a genetic test for the variant, which would allow at-risk people to modify their diets and lifestyles long before they develop diabetes. They also plan to search for new drug targets within the biochemical pathway implicated by the gene.

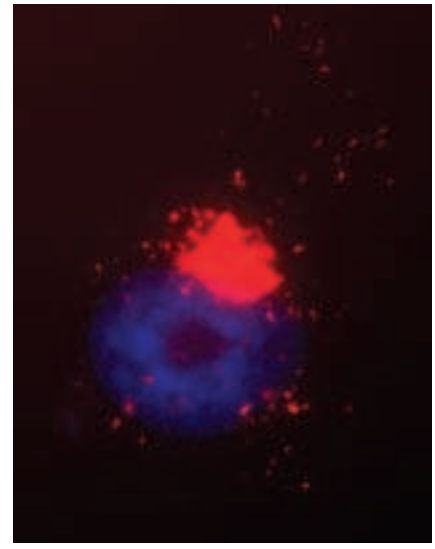
A Curious Clue to Parkinson's

Drugs that boost protein aggregation could provide a new route to treatment

SOURCE: "Pharmacological Promotion of Inclusion Formation: A Therapeutic Approach for Huntington's and Parkinson's Diseases"
Ruth Bodner et al.
Proceedings of the National Academy of Sciences 103(11): 4246–4251

RESULTS: Ruth Bodner, a postdoc at MIT's Center for Cancer Research, biology professor David Housman, and colleagues have identified a compound that can increase protein aggregation in cellular models of Parkinson's and Huntington's disease. When treated with the compound, called B2, Parkinson's cells that normally would have died survived. And Huntington's cells treated with the compound had better-functioning proteosomes—the cellular "garbage cans" that are often dysfunctional in the disease.

WHY IT MATTERS: Abnormal aggregations of protein are a characteristic of many types of neurodegenerative disease, including Huntington's, Parkinson's, and Alzheimer's. However, there is continuing scientific disagreement over the nature of these aggregations. While they correlate with some aspects of the diseases, recent evidence suggests that they may be harmless or even helpful in preventing neurotoxicity. The MIT study builds on this last possibility by demonstrating that increased protein aggregation can improve the health of cells modeling neurodegenerative disease.



Promoting the aggregation of misformed Huntingtin proteins (red) could help cells.

RUTH BODNER/MIT

METHODS: Scientists conducted a large-scale drug screen, examining how different compounds affected cells that had been engineered to produce mutant proteins implicated in Parkinson's disease and Huntington's disease.

NEXT STEP: The MIT researchers conducting the experiments would like to figure out how the B2 compound works. Cells usually get rid of misshapen proteins by breaking them down in proteosomes, but this mechanism may get overloaded in neurodegenerative disease. Housman and Bodner theorize that the compound works by helping the cell sequester into clumps the single proteins or smaller aggregates of proteins that might be harmful to it.

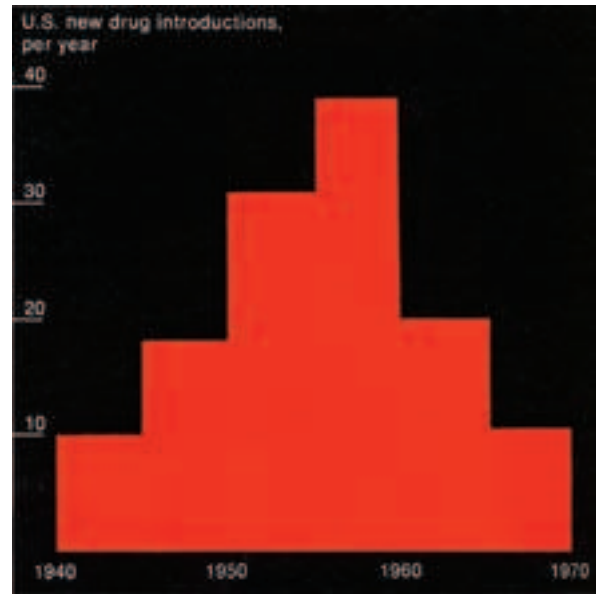
Alumni-to-Alumni Directory

Classifieds

The Elusive Nature of Drug Discovery

Understanding how drugs work has never been easy.

By Jessica B. Baker



Since 2000, the U.S. Food and Drug Administration has reported a general decrease in the number of new molecular entities—drugs with new chemical structures—submitted for approval each year, indicating a decline in the discovery of new drugs. Thirty-six years ago, pharmaceutical professionals also worried about drug discovery and lamented a decline in the rate at which new drugs were reaching the U.S. market. In December 1970, *Technology Review* published "Drugs: Has the Age of Miracles Passed?…and Will That of Science Ever Dawn?" It was a two-part review of a symposium on drug discovery at the American Chemical Society's national meeting that year. Barry M. Bloom, a representative from Pfizer, presented data, summarized in the bar graph shown here, demonstrating a decline in the rate of drug discovery.

In 1962 the Food, Drug and Cosmetic Act was amended to require that any new drug should be not only safe but efficacious. Since 1962, Mr. Bloom finds, there has been a marked tendency for new drugs to be either antibiotics, cancer treatments, or neural agents, to the neglect of the general run of diseases. In his view, discovery goes on very much as it used to, but the only drugs that reach the U.S. market are those for which an efficacy demonstration is relatively easy.

The section concludes that *it now costs about six times as much to discover a new drug, saleable in the U.S., as it did ten years ago. (Francis J. Blee, of Drexel Harriman Ripley, Philadelphia, produced the following figures: research and development investment per "new entity" between 1956 and 1962—$4.1 million; between 1963 and 1969, $23.1 million.) There is therefore a keen interest in the question of which methods of finding drugs are likely to work.*

Of equal concern is how these drugs function within the human body. In this month's Q&A *(see p. 36)*, Harvard University computational biologist George Church discusses the impact of scientific breakthroughs such as high-throughput gene sequencing on our understanding of biological systems. Church believes the day is near when drugs will be engineered to recognize tumors and individuals can affordably have their genomes sequenced, revolutionizing personal medical treatment. In the second part of the 1970 article, scientists dreamed of such increased knowledge of biology and the potential impact on drug discovery while recognizing the gaps in their era's science.

Finding new drugs is a form of professional gambling: some people think they have a system. William P. Purcell of the University of Tennessee holds that "from a philosophical point of view, one can reason that if we have the resources, such as manpower, knowledge, sophisticated instrumentation, computers, etc., to bring a successful 'moon walk' to fruition, one would anticipate that a molecule could be tailor made to be effective against a specific disease."

Dr. Purcell is for designing drugs for specific purposes, applying computers to the correlation of biological activity with chemical structure. He admitted, though, that "one knows more about the molecular structure of an isolated molecule from instrumental analyses than about the specific interaction of this molecule with a complicated biological system.… The level of sophistication of handling simultaneous equations is greater than the understanding of a parameter from pharmacological testing."

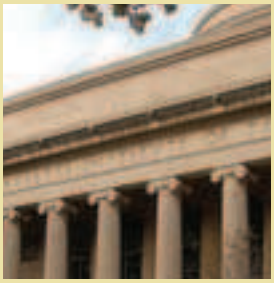
John J. Burns, of Hoffman-La Roche, Nutley, N.J., spoke of a related shortcoming which he called the "biological knowledge gap": a lack of basic understanding of disease processes and of what drugs actually do. For finding new drugs, the random synthesis of compounds, followed by screening for biological activity, is still worthwhile, as long as the biologists are good ones, and as long as they talk to the chemists. TR

Technology Review (ISSN 1099-274X), Reg. U.S. Patent Office, is published bimonthly (except in February 2006) by the Massachusetts Institute of Technology. Entire contents ©2006. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Printed by Brown Printing Company, Waseca, MN. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: send address changes to Technology Review, Subscription Services Dept., PO Box 420005, Palm Coast, FL 32142, or via the Internet at www.technologyreview.com/customerservice. Basic subscription rates: $34 per year within the United States; in all other countries, US$47. Publication Mail Agreement Number 40621028. Send undeliverable Canadian copies to PO Box 1051, Fort Erie, ON L2A 6C7. Printed in U.S.A. ABC audited

Technology Review's
Emerging Technologies Conference at MIT

September 27-28, 2006 ▪ MIT Campus





2006 Keynote Speakers:

Jeff Bezos
Founder and CEO, Amazon.com

Marc Chapman
Global Leader, Strategy & Change Practice, IBM

Jonathan Miller
Chairman and CEO, AOL

Roger McNamee
Co-founder and General Partner, Elevation Partners

Phillip Sharp
Nobel Laureate; Professor, Center for Cancer Research, MIT

Jay Walker
President, Walker Digital; Founder, Priceline.com

Discover the transformative technological innovations that will fuel tomorrow's growth.

Technology Review's Emerging Technologies Conference at MIT showcases the technologies that are poised to make a dramatic impact on our world. This unique event brings together world-renowned innovators and leaders to discuss the most important emerging technologies from around the world and how to make them matter.

Now in its sixth year, this annual two-day event features a mixture of keynote speakers, insightful panels, and groundbreaking presentations—of a caliber only Technology Review can deliver—combined with networking opportunities and live demonstrations. If you are in charge of the strategic direction of your organization or simply passionate about technology, this is an event you cannot afford to miss.

Sign up now and save $300. Visit:
www.technologyreview.com/events/tretc

Interested in Exhibiting at the Emerging Technologies Showcase or Becoming a Sponsor?
Contact Vincent Caprio at 203-733-1949 or email: Vincent.Caprio@technologyreview.com

Russia, Iran and Qatar have 58% of the world's natural gas reserves.

The U.S. has 3%.

So what does that mean for us?